

K2D3SCH1 - CORRECTED

1 UNITED STATES DISTRICT COURT
2 SOUTHERN DISTRICT OF NEW YORK

-----x

3 UNITED STATES OF AMERICA,

4 v.

S2 17 Cr. 548 (PAC)

5 JOSHUA ADAM SCHULTE,

6 Defendant.

Trial

7 -----x

New York, N.Y.
February 13, 2020
9:00 a.m.

9 Before:

10 HON. PAUL A. CROTTY,

11 District Judge
-and a jury-

12 APPEARANCES

13 GEOFFREY S. BERMAN

14 United States Attorney for the
Southern District of New York

15 BY: MATTHEW J. LAROCHE

SIDHARDHA KAMARAJU

16 DAVID W. DENTON JR.

Assistant United States Attorneys

17 SABRINA P. SHROFF

18 JAMES M. BRANDEN

Attorneys for Defendant

-and-

19 DAVID E. PATTON

Federal Defenders of New York, Inc.

20 BY: EDWARD S. ZAS

Assistant Federal Defender

21 Also Present: Colleen Geier

22 Morgan Hurst, Paralegal Specialists

Achal Fernando-Peirís, Paralegal

23 John Lee, Litigation Support

Daniel Hartenstine

24 Matthew Mullery, CISOs, Department of Justice

K2D3SCH1 - CORRECTED

(In open court; jury not present)

THE COURT: Good morning. We're still missing some jurors, David?

THE DEPUTY CLERK: Let me doublecheck, but yes.

THE COURT: Where's Mr. Branden today?

MS. SHROFF: I'm sorry, I couldn't hear you, your Honor.

THE COURT: Where is Mr. Branden today? He was not here yesterday.

MS. SHROFF: He was not here yesterday, and he will be here shortly, your Honor.

THE COURT: All right. I read the government's letter of February 12. It came into chambers last night around 5 o'clock. Attached to it was a memorandum from the director of officer security at the CIA recommending the imposition of administrative leave on Michael. That was done on August 19.

The question I have for you, for the government, is when did the government, the U.S. attorney's office find out that Michael was on administrative leave?

MR. KAMARAJU: We knew at the time, your Honor.

THE COURT: At the time?

MR. KAMARAJU: We did.

THE COURT: Do you know who wrote the CIA memo?

MR. KAMARAJU: I don't know the individual who wrote it. We referenced the group who wrote it, but I don't know the

K2D3SCH1 - CORRECTED

1 name of the individual who specifically drafted it.

2 THE COURT: Why did the government wait six months to
3 give out the information that Michael was on administrative
4 leave?

5 MR. KAMARAJU: Your Honor, I think in our view we
6 thought the relevant information was the underlying material
7 that showed the underlying conclusions about his credibility,
8 and we produced those far in advance. That was our view. We
9 produced the --

10 THE COURT: You made a judgment that there was already
11 enough information for all the cross-examination that the
12 defendant wanted to do?

13 MR. KAMARAJU: We did, your Honor. As we've done in
14 other cases, we made that determination. If we erred in that,
15 we apologize, your Honor. We made sure that -- we apologize.
16 We did believe Ms. Shroff had, among other things, the notes
17 that led to immediately preceding being put on administrative
18 leave, she had contacted his lawyer.

19 THE COURT: With regard to the notes of your meeting
20 with Michael, on August 16, why there was no 302 prepared?

21 MR. KAMARAJU: Because those were attorney notes. The
22 FBI didn't take those notes; the prosecutors took them.

23 MS. SHROFF: Did the Court want to take a copy of the
24 notes provided to us on August 16?

25 THE COURT: August?

K2D3SCH1 - CORRECTED

1 MS. SHROFF: The August 16 meeting with the
2 prosecutors.

3 THE COURT: I have the notes.

4 MS. SHROFF: I didn't know if you had them, your
5 Honor. I'm sorry.

6 THE COURT: I do have the notes. They're in the 3500
7 material, aren't they?

8 MR. KAMARAJU: Yes, your Honor. We produced them to
9 the defense.

10 THE COURT: I'm going to direct that the document
11 which led to Michael's being placed on administrative leave, it
12 is a four-page document, be produced to the defendant.

13 MR. KAMARAJU: Understood, your Honor. We'll give
14 them a copy.

15 THE COURT: All right. Anything else?

16 MS. SHROFF: Will that be now or after my cross -- I'm
17 just joking.

18 MR. KAMARAJU: We're getting it.

19 MS. SHROFF: I was just teasing you, I'm sorry.

20 THE COURT: Anything else to take up this morning? Is
21 the jury here?

22 MR. KAMARAJU: Nothing from the government, your
23 Honor.

24 THE COURT: The jury is here.

25 MS. SHROFF: Will you give me a break -- I haven't

K2D3SCH1 - CORRECTED

1 seen the document. Can I look at it before the cross? I can
2 start now, and then when I reach a point at the end --

3 THE COURT: How long are you going to be on cross?

4 MS. SHROFF: I think I have at least 30 minutes before
5 I read this four-page memo. I don't know what the four-page
6 memo is. But you can let me finish, and then I will leave that
7 part at the very end. Would that help?

8 THE COURT: Yes. Anything to get us started.

9 MS. SHROFF: That's fine. We can get started, your
10 Honor.

11 THE COURT: Are you going to bring Michael in? As
12 soon as Michael comes in, bring the jury in.

13 (Continued on next page)
14
15
16
17
18
19
20
21
22
23
24
25

K2D3SCH1

Michael - Cross

1 (Jury present)

2 THE COURT: Good morning. Please be seated. Michael,
3 I want to remind you, you're still under oath.

4 THE WITNESS: Thank you.

5 THE COURT: Ms. Shroff.

6 MICHAEL,

7 CROSS-EXAMINATION (Continued)

8 BY MS. SHROFF:

9 Q. March 16 is when you first met with the FBI for the first
10 time, March 16, 2017?

11 A. I don't remember the date.

12 Q. During that interview, did you tell the FBI, when they
13 asked you about Mr. Schulte, that you had seen no -- that you
14 had seen Mr. Schulte go through a rough time at the end of his
15 employment with EDG?

16 A. I don't remember the specific words, but I remember
17 something like that.

18 Q. I'm going to give you 3550-01, and if you want to refer to
19 it to refresh your recollection, feel free to do so, okay?

20 A. Thank you.

21 Q. You also told them, when they asked you, if you had -- you
22 said to them that you had seen no alerting behavior from
23 Mr. Schulte. Correct?

24 A. I don't see this in the highlights.

25 Q. Okay. Do you recall telling them that while you thought

K2D3SCH1

Michael - Cross

1 Mr. Schulte might have been unhappy or disgruntled, that there
2 was no other behavior that you saw that concerned you?

3 Take a look at page two, would you, the second
4 paragraph. I may have forgotten to highlight it. It is the
5 third line.

6 A. Yes, I see it.

7 Q. Okay. So you recall now saying that to the FBI?

8 A. It's in this document, yes.

9 Q. And the document is a writeup of a meeting with you, right?
10 If you take a look at the front page.

11 A. Yes, this seems to be a summary of our -- of my meeting
12 with the FBI.

13 Q. Okay. They asked you, did they not, the FBI, about
14 Mr. Schulte's foreign travel?

15 A. I don't remember.

16 Q. And is it fair to say that you knew Mr. Schulte not to be a
17 good traveler?

18 A. Or he didn't like to travel?

19 Q. Foreign travel.

20 A. Right.

21 Q. You told them that he wasn't big on foreign food or foreign
22 travel?

23 A. Right, he didn't like it. But how good he is at it, I
24 don't know.

25 Q. Fair enough. But you told them he didn't like foreign

K2D3SCH1

Michael - Cross

1 travel, right?

2 A. That is a true statement. I don't know if -- I don't
3 remember saying that.

4 Q. Okay. You know it to be true also that you think
5 Mr. Schulte was reliable, correct?

6 A. Yes.

7 Q. And thought he was hard working, correct?

8 A. Yes.

9 Q. And is it fair to say that you told the FBI that you and
10 others at the CIA had talked about the Snowden incident,
11 correct?

12 A. Me and co-workers did talk about the Snowden incident, yes.

13 Q. You told the FBI, did you not, that when the Snowden
14 incident occurred, everyone at the FBI talked about how that
15 could also happen to Confluence, correct?

16 A. At the FBI?

17 Q. I mean at the CIA.

18 A. At the CIA, yes.

19 Q. You all talked about it, right?

20 A. I don't remember if we specifically mentioned Confluence.
21 But we definitely said something like this could happen here.

22 Q. Take a look at page three of three, would you. See if that
23 refreshes your recollection that you said people at EDG said
24 the same thing could happen to Confluence.

25 A. Do you have a paragraph?

K2D3SCH1

Michael - Cross

1 Q. Sure. Page three, second paragraph, last line.

2 A. Yes, I see it here.

3 Q. Right. Do you recall Mr. Schulte telling you that he had
4 quite a few expletives about Mr. Snowden, and he thought he was
5 a traitor?

6 A. Yes.

7 Q. You also told the FBI, did you not, that access to DevLAN
8 was, I quote, broad.

9 A. Sorry, can you repeat the question?

10 Q. Sure. Broad, B-R-O-A-D.

11 A. I don't remember saying that. But, yeah. People -- as
12 long as you were a developer, you could get access to DevLAN.

13 Q. Could you put that piece of paper, you can set it aside.
14 There you go.

15 Did the FBI insinuate to you at that time that because
16 Mr. Schulte was unhappy or disgruntled at the CIA, he would be
17 the person who would have done this?

18 A. I don't remember these meetings. They're very -- they're
19 very blurry. But, it was clear that they had an interest in
20 him because of all the things that had happened prior to him
21 leaving.

22 Q. Is it fair to say that others at the CIA also thought that,
23 because he was unhappy at the CIA, he would be the one to do
24 this?

25 A. I think that was the general assumption.

K2D3SCH1

Michael - Cross

1 Q. Right?

2 A. I can't think of anyone in specific that told me that, but,
3 I feel like there was that feeling, yes.

4 Q. Right. And that assumption was passed on to the FBI every
5 time the FBI interviewed anyone at the CIA, correct?

6 A. I don't know what the other interviews went like.

7 Q. Okay. When the FBI was interviewing you for the first
8 time, they asked you about Mr. Schulte's family, correct?

9 A. I don't remember.

10 Q. You don't remember them asking you if you'd ever met his
11 parents, his mother and father?

12 A. Yeah, I don't remember that specific question.

13 Q. It's on the handwritten 302 on page two of six.

14 Do you by any chance remember telling them that you
15 had not met his parents, but that you knew he was from Texas?

16 A. I don't remember the specific questions, but that is a true
17 statement.

18 Q. Just go to page two. And then you told them, did you not,
19 that as far as you knew, Mr. Schulte liked the United States
20 government, correct?

21 A. I don't remember saying this, but that's true, yes.

22 Q. Right. And you told them that, in fact, what he wanted to
23 do was to kill the terrorists, correct?

24 A. I don't remember saying this, but, he -- he definitely had
25 some colorful things to say about terrorists.

K2D3SCH1

Michael - Cross

1 Q. And he also told you repeatedly, did he not, that in his
2 opinion, America was the best country?

3 A. Yes.

4 Q. And the FBI asked you if you knew Mr. Schulte to attend any
5 rallies or protests; do you remember that?

6 A. I do not remember that.

7 Q. Okay. Do you recall Mr. Schulte -- take a look on page
8 four of six, okay, the first full paragraph, the last line.

9 THE COURT: What's the exhibit number you're working
10 with?

11 MS. SHROFF: I'm working with, your Honor, 3550-03,
12 page four. Do you have it?

13 THE COURT: I've got it, thank you.

14 Q. Does that refresh your recollection?

15 A. Yes, it's stated here in the document. I can't read that
16 last line.

17 Q. "No rallies or protests" is how I read it.

18 A. Right. No rallies or protests. And that's true, I still
19 to this day don't know of any rallies or protests that he
20 attended.

21 Q. Then they talked to you about your involvement in helping
22 him move from Virginia to New York, correct?

23 A. Yes.

24 Q. They asked you a whole series of questions as to how you
25 came about to help him move, correct?

K2D3SCH1

Michael - Cross

1 A. Yes.

2 Q. And they asked you why you helped him move, correct?

3 A. I don't remember specific questions, but I do remember
4 questions about helping him move.

5 Q. And you explained to them that it was like a coincidence,
6 right? You'd already planned a trip with another friend, he
7 was moving at the same time, he needed help loading up luggage
8 and moving stuff, correct?

9 A. Yes.

10 Q. It was not preplanned, right? It just happened, right?

11 A. Yeah.

12 Q. You told them that you had already planned to do this with
13 another friend, right?

14 A. Yes.

15 Q. And then they asked you about that friend, correct? They
16 asked you what the name of the friend was, correct?

17 A. Yes.

18 Q. Then they asked you for your friend's number, correct?

19 A. I don't remember specifically what information they asked
20 for.

21 Q. We'll come back to that if we need to. Let's move to the
22 next point.

23 They then asked you if Mr. Schulte had left any stuff
24 with you, correct?

25 A. Yes.

K2D3SCH1

Michael - Cross

1 Q. You told them that he had, correct?

2 A. Yes.

3 Q. It was normal, everyday stuff he left with you, correct?

4 A. I wouldn't say it's normal. It was a lot of furniture. So
5 I don't think that's normal.

6 Q. Oh, to have a -- I agree with you there. But it was
7 furniture, right? It was nothing unusual?

8 A. Right, yeah, the actual things were not unusual.

9 Q. Okay. And he had a lot of servers in his house? You
10 visited his house in Virginia, right?

11 A. I did visit his house. He had a lot of computers.

12 Q. He played a lot of League of Legends or something?

13 A. Yes.

14 Q. Some kind of game?

15 A. Yes, it's a video game.

16 Q. A lot of men, people play it; is that right?

17 A. It has a large user base.

18 Q. It is some kind of online game where you pretend to have
19 avatars and kill each other online or something like that?

20 Is that right, basically?

21 A. Yes.

22 Q. And you played that game, did you not, with Mr. Schulte?

23 A. Yes.

24 Q. And then there was some other cousin of his, Mr. Miller,
25 Justin Miller would played that game, correct?

K2D3SCH1

Michael - Cross

1 A. That's not a cousin of his.

2 Q. Is that somebody who played another game with him?

3 A. Yes.

4 Q. And somebody named Shane who played that game with all of
5 you?

6 A. Yes.

7 Q. And you all went online with your little headset and played
8 that game after work, correct?

9 A. Yes.

10 Q. You told the FBI that he had a lot of servers in his home,
11 correct?

12 A. I don't remember specifically saying that.

13 Q. Okay. And at that point in time during that interview, do
14 you remember if they asked you about your use of Confluence?

15 Do you remember if they asked you?

16 A. I think so, yes.

17 Q. How about your use of Stash?

18 A. I don't remember.

19 Q. How about Jira?

20 A. Yeah, I think the questions were broad about the Atlassian
21 suite. I don't know if they got into specific ones. Maybe
22 they did.

23 Q. Let's turn to your next meeting with the FBI which was on
24 June 8th of 2017, okay. This is your second interview with
25 them, right? And at this time, they are still just simply

K2D3SCH1

Michael - Cross

1 asking you questions, correct?

2 A. I don't remember the second meeting.

3 Q. I'm sure you don't. Trust me, it's been a while, so I
4 understand that completely.

5 But you met with them a second time, right?

6 A. Yes.

7 Q. And again during that meeting they didn't ask you about any
8 other person other than Mr. Schulte, correct?

9 A. I don't know.

10 Q. You don't know?

11 A. I don't remember.

12 Q. Okay. Let's give you 3550-04, and I think I highlighted
13 for you so it will go easier.

14 A. Thank you.

15 Q. It was during this meeting that you told them about
16 Mr. Schulte reaching out to you after the leaks had become
17 public; correct? Do you remember that?

18 A. I remember telling them about him reaching out to me. I
19 don't remember if it was this specific meeting.

20 Q. Okay. Take a look at the highlighted portion on page one,
21 okay?

22 A. Okay.

23 Q. You told the FBI, did you not, that Mr. Schulte had sounded
24 upset to you that people thought it was he who had done the
25 leaks, correct?

K2D3SCH1

Michael - Cross

1 A. Yes. I believe the word was he seemed concerned.

2 Q. Right. You would be concerned too if somebody accused you
3 of something you didn't do, correct?

4 A. Yes.

5 Q. And you also told them that you essentially blew him off,
6 correct? You didn't want to engage and talk to him, correct?

7 A. Yes, I ignored the initial text messages. And then in the
8 phone call, I didn't want to talk about that subject.

9 Q. Okay. And at first you didn't report the fact that
10 Mr. Schulte contacted you, correct?

11 A. Correct.

12 Q. And then somehow or the other, the deputy chief of EDG said
13 if somebody's contacted you, report it. And then you reported
14 it, correct?

15 A. Correct.

16 Q. Now, during this meeting, do you remember if the FBI showed
17 you any documents?

18 A. I don't remember --

19 Q. Okay.

20 A. -- at which meeting they showed me documents.

21 Q. But there came a point, did there not, that they showed
22 you -- let me just show it to you right now, 3550-503, and it
23 is a three-page document that consists of photos.

24 A. Thank you.

25 MS. SHROFF: Your Honor, the government agrees to

K2D3SCH1

Michael - Cross

1 introduce it as evidence as Defense Exhibit F.

2 THE COURT: F is received in evidence.

3 (Defendant's Exhibit F received in evidence)

4 MS. SHROFF: Could you pull it up for the jury.

5 Q. Do you recognize this?

6 A. Yes.

7 Q. And you recognize this to be what, sir?

8 A. This is a screenshot that the FBI showed me during one of
9 our meetings.

10 Q. You see the date on top?

11 A. On top of the screenshot or right beneath the title?

12 Q. No, no. Right there, 6/01?

13 A. Yes, I see it.

14 Q. And that's during your June 1st, 2017, meeting with the
15 FBI?

16 A. I don't remember when they showed me these documents.

17 Q. Fair enough. And you agreed that this is Mr. Schulte's
18 login page, correct?

19 A. Yes.

20 Q. Desktop of a virtual machine, correct?

21 A. Yes.

22 Q. Josh's DevLAN screen, correct?

23 A. No.

24 Q. No, it's not correct? What is it then?

25 A. This is a VM that he would have run on his DevLAN machine.

K2D3SCH1

Michael - Cross

1 Q. So it is a virtual machine that he ran on his own DevLAN,
2 correct?

3 A. Yes.

4 Q. Okay. So it says "Josh." Correct?

5 A. Yes.

6 Q. Then it says "Michael," correct?

7 A. Yes.

8 Q. And then it says "other," correct?

9 A. Yes.

10 Q. And they asked you about this document, correct?

11 A. Yes.

12 Q. And you told them, did you not, that Josh had given you
13 what you turned as a phrase "Sudo creds," correct?

14 A. I don't remember specific wording but, yes. I believe he
15 gave me Sudo accesses to this VM.

16 Q. Just if you need help, it's on page two of the document I
17 showed you before. Okay?

18 A. Okay.

19 Q. And then you told them that you probably had root access to
20 the machine to do with it what you wanted, correct?

21 A. Yes. If I had Sudo creds, then that's true.

22 Q. They asked you if you were surprised to find out that you
23 shared a VM with Josh, and you said no, correct?

24 A. Correct.

25 Q. Right. And you told them that it was normal to do this at

K2D3SCH1

Michael - Cross

1 the CIA, correct?

2 A. To do it in -- to do it in AED, at least, it's normal.

3 Q. I'm only talking about where you were, sir.

4 A. Right. CIA at large it would be very --

5 Q. You know, that's a fair point. Just in your group that you
6 were working with Mr. Schulte.

7 A. Right.

8 Q. At that time.

9 A. Yes.

10 Q. So in that group, it was very normal. You tried to explain
11 this to the FBI, correct?

12 A. Yes.

13 MS. SHROFF: You can take that down.

14 Q. Then you told them also why it was normal, correct?

15 A. I don't remember but --

16 Q. Okay. Let me see if I can help you remember. You said it
17 was normal to share, because you worked on operations together,
18 and everyone in the branch helped each other with their tools,
19 correct?

20 A. That's a true statement.

21 Q. And then you kind of added that it kind of sucked that your
22 name was on this VM, correct?

23 A. I don't remember that.

24 Q. Take a look at the first paragraph, page two of eight. It
25 sucks. I don't mean to be rude, but that's the word it says,

K2D3SCH1

Michael - Cross

1 "suck," right?

2 A. Yes.

3 Q. That your name was on the virtual machine, correct?

4 A. Correct.

5 Q. And that you understood from the FBI that that put you
6 under the microscope, correct?

7 A. Correct.

8 Q. Then you also tried again to explain to the FBI, did you
9 not, that there was nothing nefarious about this, right? That
10 this was normal to have a VM, correct?

11 A. Yeah, it says that here.

12 Q. Right. And that you told them again that this is just part
13 of the work you guys did, right? You shared VMs?

14 A. Yeah.

15 Q. Okay. And then, that's the word you used "nefarious," that
16 there was nothing nefarious about this, right?

17 A. That's the word that's in this document, yes.

18 Q. Okay. Now, they asked you, did they not, in great detail
19 about what projects you worked on with him, correct?

20 A. It does say so here, yes. I mean, I don't see that
21 specific question, but it goes on to talk about projects we
22 worked on.

23 Q. Right. Is it fair to say, sir, that when you were talking
24 to them, there was a lot of stuff you didn't remember even back
25 then, right?

K2D3SCH1

Michael - Cross

1 A. Right.

2 Q. And then you told them, look, if you want, I can follow up
3 and get you the answers, because they seemed to be really
4 interested in these answers, correct?

5 A. I do remember following up, yes.

6 Q. Right. And then when you told them you could only remember
7 two projects, they told you to follow up with them and give
8 them the names of the other projects, correct?

9 A. I'm sure it says that here.

10 Q. Okay. But it would be a normal thing, right? If they
11 asked you something you couldn't remember, you said, "I'll
12 follow up and give it to you," right?

13 A. Yes.

14 Q. Now, during this same interview, which is still June of
15 2017, seems like a very long interview because it's -- but they
16 asked you about the use of hard drives, correct?

17 A. I don't remember.

18 Q. Take a look at page two, second-to-last paragraph.
19 Penultimate paragraph over there. It starts with "later."

20 A. I see it.

21 Q. Then they asked you of all things about hard drives you had
22 bought for him on Amazon. Do you remember that?

23 A. I do.

24 Q. Right. And you explained to them that it was perfectly
25 benign that you bought hard drives for him on Amazon, correct?

K2D3SCH1

Michael - Cross

1 A. In this specific case.

2 Q. Right. We're only talking -- was there ever a case where
3 you bought him hard drives that you did not think was benign?

4 A. I only ever bought him hard drives this one time. But the
5 reason, like, I wouldn't normally just buy him hard drives, I
6 would have told him to buy it himself. But the reason was
7 there was some deal going on, and so he's like, if I buy it and
8 then you buy it, we all get the deal and I'll just pay you
9 back.

10 Q. Right. It's normal, right?

11 A. Yeah.

12 Q. Yeah. Amazon had a cap on the sale, like everyone could
13 only get two, and he wanted four or something like that?

14 A. Yes, it was something along those lines.

15 Q. I want to make sure I understand this. You told the FBI
16 that when Mr. Schulte asked you to buy these hard drives for
17 him, he gave you his credit card so that the purchase would be
18 tracked to his credit card, correct? Take a look at that
19 paragraph. You see that?

20 A. Yes.

21 Q. Okay. And then also the hard drives were actually
22 delivered to Mr. Schulte's house. It's not like they came to
23 your house and then you gave them to Mr. Schulte, right?

24 A. Correct.

25 Q. Right. Okay. They had brought with them a printout of

K2D3SCH1

Michael - Cross

1 the Amazon purchase, correct? Do you remember that?

2 A. The FBI?

3 Q. Yeah.

4 A. No, I don't remember that.

5 Q. Okay. Do you remember that during this interview, they
6 made you drive off site so that could you pick up your e-mail
7 and show them this Amazon purchase on your e-mail?

8 A. I remember driving off site to show them things. The
9 e-mail could have been one of them.

10 Q. Okay. And during this interview, they covered topics that
11 they had covered already. They re-covered the fact that you
12 helped him move to New York, correct? Just flip the page over.

13 A. Yes, I see that here.

14 Q. Okay. And then you gave them all of the details again as
15 to how you came to share a ride and went to New York with him,
16 correct?

17 A. Yes.

18 Q. And again, there was nothing nefarious about that at all,
19 correct?

20 A. Correct.

21 Q. Okay. And then you told them that you had spoken to him
22 since he had started work at Bloomberg, correct?

23 A. Correct.

24 Q. And that he had told you, and then you had told the FBI,
25 that life at Bloomberg was good, correct?

K2D3SCH1

Michael - Cross

1 Take a look at three of eight at the bottom. It's
2 highlighted.

3 Do you recall him telling you he found his new job
4 interesting, correct?

5 A. Yes, I said that.

6 Q. He joked about how he thought it was kind of cool for him
7 to be at Bloomberg and be known he had worked at the CIA?

8 A. I do remember him mentioning that being on his profile.

9 Q. He told you, right, that he missed the mission, he didn't
10 have a lot of friends in New York yet, but he was doing okay at
11 Bloomberg, right?

12 A. Yes, I remember the not having a lot of friends in New York
13 yet.

14 Q. He had just moved here, correct?

15 A. Yes.

16 Q. And anyway, like many other developers, he had a hard time
17 making friends, correct?

18 A. Yes.

19 Q. The FBI asked you about Mr. Schulte's financials, correct?

20 A. Do you have a cite? I don't remember a specific question
21 about his financials.

22 Q. Okay, I'll make it easier. Do you recall them asking you
23 if he ever used bitcoin?

24 A. No, I don't recall.

25 Q. I'll get to that in a minute. But as far as you knew, you

K2D3SCH1

Michael - Cross

1 never saw Mr. Schulte live above his means, correct?

2 A. No.

3 Q. And then they spoke again about the security about DevLAN,
4 correct?

5 A. Do you have a cite? I don't remember a specific question.

6 Q. Take a look at page four. Let me move forward from that.

7 A. Okay.

8 Q. And then they talked -- they asked you about his
9 relationship or his impression of Karen, correct?

10 A. Of caring?

11 Q. Karen. K-A-R-E-N, Karen?

12 A. Oh.

13 Q. Do I have that name wrong?

14 A. I don't remember that question. I thought you said the
15 word caring, C-A-R-I-N-G, and I didn't remember that question
16 either.

17 Q. Do you see -- does that remind you?

18 A. I don't remember a question about Karen.

19 Q. Okay.

20 A. I see it at the bottom.

21 Q. Take a look at five of eight. Do you see the top paragraph
22 on page five?

23 A. Yes, I see that, the last two sentences of page four and
24 pulls over to page five.

25 Q. Right. And he told you, did he not, that he thought she

K2D3SCH1

Michael - Cross

1 was just trying to get promoted, correct?

2 A. I remember that his sentiment of Karen was she was not
3 taking his report seriously.

4 Q. Right. And she was just trying to get promoted, correct?

5 A. I don't remember him specifically saying that, but I know
6 he thought she was not taking this seriously, just wanted to
7 ignore this, and just wanted this to go away.

8 Q. Does it not refresh your recollection about trying to get
9 promoted? You see it's crossed out by the line?

10 A. Oh yeah, I wasn't looking at that because it's crossed out.

11 Q. It's just he typed it too close to the line.

12 A. Okay. It does say here to get promoted, so he is willing
13 to go over her head until someone would listen to him.

14 Q. Right. And he expressed to you his frustration about not
15 being heard by Karen, correct?

16 A. Yes.

17 Q. He thought because Karen and Mr. Weber were friends or
18 friendly, she tended to listen to Mr. Weber and not him?

19 A. Yes.

20 Q. You told this to the FBI, right?

21 A. That is a true statement.

22 Q. And you did your best to explain the dynamics of the CIA to
23 the FBI, because that's what they were asking you about,
24 correct?

25 A. I answered the questions the best I could.

K2D3SCH1

Michael - Cross

1 Q. Right. I mean, you had no control over what they wrote
2 down, but you answered their questions to the best of your
3 ability, correct?

4 A. Yes.

5 Q. During the same interview -- you can put that down. You
6 told them about Josh Schulte's love of movies, correct?

7 A. I don't remember this.

8 Q. Okay. Is it fair to say he liked movies?

9 A. Yes.

10 Q. He had a ton of movies, correct?

11 A. Yes.

12 Q. And he had something called movie night?

13 A. Yes.

14 Q. He was into getting some kind of Torrent site called "pass
15 the popcorn"?

16 A. Yes.

17 Q. I'm not even going to ask you what a Torrent site. It is
18 to watch movies, "pass the popcorn"?

19 A. Yes, he was passionate about joining this, I don't know
20 this Torrent site.

21 Q. And when he had these movies, he shared them with everyone
22 at the CIA -- not everyone, I mean in your friend group. Not,
23 you're right, not the whole CIA.

24 A. Yes. People who wanted access, he would give them access.

25 Q. Freely, right?

K2D3SCH1

Michael - Cross

1 A. Yes.

2 Q. He never hassled anyone and said, oh, I'm paying for the
3 site, so you pay me. Nothing, right? Just give it to them?

4 A. Correct.

5 Q. You remember the FBI asking you if Mr. Schulte was a
6 vigilante hacker by night? Do you remember that phrase they
7 used?

8 A. I think I do actually, yes.

9 Q. You told them, no, you didn't know him to be a vigilante
10 hacker at night?

11 A. Correct.

12 Q. You in fact did not know him to be a vigilante hacker at
13 night.

14 A. Correct. I did not know him to be a vigilante hacker.

15 Q. If you look at page six of 3550-03 is where they ask you if
16 he was ever using bitcoin. And you said no.

17 A. Do you have the paragraph?

18 Q. I'm sorry?

19 A. Do you have the paragraph?

20 Q. Sure. Let me just help you here.

21 MR. KAMARAJU: At some point I'm going to ask that the
22 defense counsel stop reading from the document.

23 MS. SHROFF: Okay.

24 Q. Put it down, it's okay.

25 You don't remember that question?

K2D3SCH1

Michael - Cross

1 A. No.

2 Q. That's all right. Do you remember the FBI asking you about
3 Mr. Schulte's use of various software programs, including Tor
4 and Tails?

5 A. I do remember Tor. They asked if he had used Tor before.

6 Q. Right. And you told them that he never kept it a secret
7 that he had used Tor before, correct?

8 A. Correct.

9 Q. In fact, his group joked about the fact that he used Tor,
10 correct?

11 A. Yes, him and Jeremy had a discussion about it.

12 Q. Right. But they also mocked him, correct, like in a
13 good -- I don't mean in a negative way. Just in a joking way,
14 they told him to get off and stop using Tor?

15 A. Yes. Jeremy said it was -- you were supporting bad things
16 and you shouldn't use Tor.

17 Q. But Jeremy knew he was using Tor, right?

18 A. Yes.

19 Q. And Jeremy -- that's Jeremy Weber, right?

20 A. Yes.

21 Q. The man that he and Mr. Schulte didn't quite get along,
22 correct?

23 A. Correct.

24 Q. And Mr. Weber thought -- I'm going too fast.

25 Mr. Weber thought that he should be able to tell

K2D3SCH1

Michael - Cross

1 Mr. Schulte what to do, correct?

2 A. Yes, Mr. Weber --

3 Q. Mr. Schulte thought that he should not be able to do that,
4 correct?

5 A. Correct.

6 (Counsel conferring)

7 Q. Was it at this meeting that the FBI tried to convince you
8 to wire yourself up and call or text Mr. Schulte?

9 A. No, they never tried to convince me of this.

10 Q. Did they ask you?

11 A. I believe that I had made the statement, you know, I -- I
12 don't remember the specific wording, but I feel like I had
13 actually brought this up, and then at the end of the meeting,
14 they asked me would you do that.

15 Q. Okay. And you said you would first want to see what proof
16 the FBI had linking Mr. Schulte to these leaks, correct?

17 A. Yes, I would want -- yes.

18 Q. And they never followed up after that, right?

19 A. Correct.

20 Q. And by the way, was it also in this meeting that they asked
21 you to take a limited polygraph or was that later?

22 A. I don't remember which meeting that was in.

23 Q. Okay. We'll get back to that later then. They asked you,
24 did they not, about a meeting that you -- not a meeting, but
25 they asked you about a time that you went into work on a

K2D3SCH1

Michael - Cross

1 weekend; is that right?

2 A. I do remember a question about that.

3 Q. Right. They had known you had gone in on a weekend, and
4 they asked you about it, right?

5 A. Yes.

6 Q. You again explained to them that it was nothing nefarious
7 to go into work on a weekend?

8 A. Yeah. I don't remember the specific words, but it was
9 normal to go in if you had to get something done.

10 Q. Right. In fact, sometimes people went to talk about -- to
11 do their PARs, because it's hard to write up a PAR?

12 A. Yes, specifically I had brought that up and said one of the
13 reasons I come in on the weekend is to do my PAR.

14 Q. A PAR is a performance -- what is it?

15 A. I don't know what the acronym stands for. Something about
16 our performance review. It's how you -- you write up how you
17 think you've done for the year.

18 Q. Personal Appraisal Review maybe?

19 A. Something.

20 Q. Something like that?

21 A. Yeah. It's your push for promotion.

22 Q. Okay. And at first you thought that you had gone in to
23 write a PAR, correct?

24 A. Yes.

25 Q. But then you realized you'd actually gone into work on a

K2D3SCH1

Michael - Cross

1 project, correct?

2 A. Yes. Well, this is one of those where I said, you know, my
3 best guess is I came in to work on my PAR, but I will follow up
4 with you. I save all my PARs so I went, looked at the time
5 stamps on the PARs, none of those were during that date. So
6 then I went back to other, we had to fill out these weekly
7 activity reports that say kind of what we did for the week, so
8 I looked at that. And I was like I must have been working on
9 this project.

10 Q. Right. And you followed up, you did all of that, and you
11 told that to the FBI, right?

12 A. Yes.

13 Q. They asked you about that weekend because Mr. Schulte also
14 happened to be working that weekend?

15 A. They mentioned that, yes.

16 Q. Did you think it was odd that Mr. Schulte was working that
17 weekend or did the FBI think it was odd that Mr. Schulte was
18 working that weekend or both?

19 A. At first I thought it was odd.

20 Q. Okay.

21 A. Just because --

22 Q. Go ahead.

23 A. Just because, you know, although it was normal to come in
24 on the weekend, it was less common -- rare, I would say, to
25 come in on the weekend. One of us probably would have told

K2D3SCH1

Michael - Cross

1 each other, you know, we were going to come in on the weekend.

2 But then I looked at my situation, I was like, well, I
3 didn't tell him I was coming in, so I guess this is normal.

4 Q. Okay. You told that whole story to the FBI, right?

5 A. I don't remember.

6 Q. You met with them again after that. That meeting was June,
7 then you met with them in August, right? August 30, 2017?

8 A. I don't remember the date.

9 Q. That's fine. And I just want to make sure that the record
10 is clear. At that time you're not on administrative leave,
11 right? You're still a full-time CIA employee?

12 A. Correct.

13 Q. And again, they asked you a whole slew of questions,
14 correct?

15 A. Yes.

16 Q. And it is in this meeting, if you remember, that you told
17 the FBI that, in your opinion, Mr. Weber was setting
18 Mr. Schulte up. Do you remember that?

19 A. I remember feeling that way.

20 Q. Okay. By that you mean that you thought Mr. Weber was
21 setting Mr. Schulte up to fail at his job at the CIA, right?

22 A. I thought he was -- baiting him into using his accesses,
23 for a lack of a better word.

24 Q. Did you say "baiting"?

25 A. Yes.

K2D3SCH1

Michael - Cross

1 Q. B-A-I-T-I-N-G?

2 A. Yeah, I thought he was setting -- he was creating
3 circumstances where he knew that Josh had access to change
4 permissions on the server, Josh was an admin. He was telling
5 Josh you cannot do this. But Josh technically could do that,
6 right, he had the technical capability to do that. So, Josh
7 was going to do that.

8 Q. Okay. You told Mr. Weber your concern?

9 A. Yes.

10 Q. And Mr. Weber said butt out, correct?

11 A. Yes, in summary. Mr. Weber said butt out.

12 Q. By then Mr. Schulte had actually confided in you -- he
13 confided in you, you were friends, right?

14 A. Yes.

15 Q. He told you, right, that he felt hassled by that memo of
16 warning, correct?

17 A. Yes, yes.

18 Q. Thought it was unfair, correct?

19 A. Yes.

20 Q. And you felt that Mr. Weber was trying to punish
21 Mr. Schulte, correct? That's the word you used for the FBI?

22 A. I don't remember using that word.

23 Q. Okay. Did you tell the FBI that you felt that Mr. Weber
24 was trying to punish or stick it to Mr. Schulte?

25 A. I don't remember saying that.

K2D3SCH1

Michael - Cross

1 Q. Did you feel that way?

2 A. When I think back on it now, I don't know he was trying to
3 punish him as much as -- he just wanted -- he didn't think that
4 Josh should be able to make claims like "I'm the one taking
5 this project" and things like that.

6 Q. Right. They had a tussle, correct?

7 A. Yes.

8 Q. And the tussle was public, correct?

9 A. Yes.

10 Q. I mean, Mr. Weber would say things to Mr. Schulte,
11 Mr. Schulte would respond back, and it wasn't like a secret in
12 that cubicle or anyplace else, correct?

13 A. Right. I don't know that the rest of the division or the
14 rest of the group knew, but definitely within OSB it was known.

15 Q. And Mr. Weber knew that Mr. Schulte did not consider him,
16 Mr. Weber, to be a person of authority, correct?

17 A. I don't know what Mr. Weber knew.

18 Q. Fair enough. Okay. Now, you tried to suggest to
19 Mr. Weber, did you not, that he should tell Mr. Schulte clearly
20 that he was going to remove Mr. Schulte's access from the
21 libraries, correct? Do you remember that?

22 A. I remember telling him he should -- oh, from the libraries?

23 Q. You told Mr. Weber that, in your opinion, Mr. Weber should
24 tell Mr. Schulte that he was going to do something to
25 Mr. Schulte before he did it, correct?

K2D3SCH1

Michael - Cross

1 A. I remember having a discussion with Mr. Weber saying you
2 should remove his accesses. It's potentially in that
3 conversation I said, you know, and you should tell him as well.

4 Q. Okay. Let's take a look, shall we, to your -- to a 3550 if
5 you have it there. And that's page 13. 3513, page two.

6 A. Page two.

7 Q. I haven't given it to you. Sorry about that.

8 A. That's okay.

9 MS. SHROFF: Did you want a copy, your Honor?

10 THE COURT: Yes, please. Thank you. Great. Thanks.

11 A. Where am I looking?

12 Q. Just look at paragraph, there is a paragraph UU and then S.
13 Do you see that, starts with in April. Page two. You with me?

14 A. Sorry, "in April 2016"?

15 Q. Yes. Just read it to yourself. Don't read it out loud.

16 A. Okay.

17 (Pause)

18 Q. Let me know when you're ready.

19 A. Okay, I'm ready. I read the second paragraph.

20 Q. Does that refresh your recollection that in fact you told
21 Mr. Weber that you thought he was setting Josh up to get into
22 trouble?

23 A. I remember saying that to him.

24 Q. And you said that to him, and you said to him you're
25 setting him up, because everybody knew how Josh would react,

K2D3SCH1

Michael - Cross

1 correct?

2 A. Yes.

3 Q. And then you said to him that -- you were kind of even
4 Steven, right? You also told him that you thought Josh should
5 calm down, right?

6 A. Yes.

7 Q. And then you said that he should really -- by "he" I mean
8 Mr. Weber -- should really tell Mr. Schulte before removing his
9 accesses that he was going to do so. Correct? That was your
10 opinion, correct?

11 A. Yes, yes, it does say that here.

12 Q. Right. And then you also said to the FBI that back then
13 when you were not on administrative leave, it was your belief
14 that Mr. Weber was trying to punish Mr. Schulte and trying to
15 get him to violate the letter he had signed about not abusing
16 his privileges. Do you see that? I highlighted it for you.

17 A. Yes, I see it.

18 Q. Okay. You can put that aside.

19 You know of a project called Brutal Kangaroo, correct?

20 A. Yes.

21 Q. Do you remember telling the FBI in the same interview that
22 Brutal Kangaroo was a complex tool?

23 A. I saw that in that paragraph.

24 Q. Right. And it was in fact a complex tool, correct?

25 A. Correct.

K2D3SCH1

Michael - Cross

1 Q. And is it fair to say that in your opinion, at least,
2 nobody in OSB wanted to work on it?

3 A. Yes.

4 Q. Okay. But Mr. Schulte was open to working on it, correct?

5 A. Yes.

6 Q. In fact he wanted to work on it, correct?

7 A. He was the creator.

8 Q. I'm sorry?

9 A. He was the creator.

10 Q. He was the creator of Brutal Kangaroo?

11 A. Yes.

12 Q. Right. And nobody else wanted to work on it but he did,
13 correct?

14 A. Yes.

15 Q. And you told this to the FBI, and then you also told the
16 FBI that you did not think Josh would do anything to hurt the
17 agency, correct?

18 A. I don't recall. I remember telling them he wanted to work
19 on at it, I see that in here. I don't remember seeing the
20 whole agency thing.

21 Q. Okay. We'll find it in a minute.

22 A. Okay.

23 (Continued on next page)

K2dWsch2

Michael

1 BY MS. SHROFF:

2 Q. Page 3, paragraph 2.

3 MS. SHROFF: Thank you.

4 A. What does the paragraph start with? Is it "this screen,"
5 or is it --

6 Q. No. Page 3.

7 Hold on. Let me just walk to you.

8 It's item No. 1.

9 A. Item No. 1.

10 Q. Yeah.

11 A. I saw No. 2, and I just went down to that.

12 MS. SHROFF: Do you have some water up there, sir?

13 THE WITNESS: I do not, but I'm OK.

14 Thank you.

15 MS. SHROFF: Thank you.

16 Q. Do you see that phrase that you "did not think K.P. would
17 do" -- I'm reading, "that Mr. Schulte would not do anything to
18 harm the agency," correct? Does that refresh your
19 recollection?

20 MR. KAMARAJU: Your Honor, we object to the reading
21 again.

22 THE COURT: Yes. You can't read from a document
23 that's not in evidence.

24 MS. SHROFF: I'm sorry. I can highlight it for him.

25 THE COURT: Yes.

K2dWsch2

Michael

1 A. I know you pointed this out to me. I just don't see it.

2 I'm sorry. Can you point it out to me?

3 Thank you.

4 Yes, it says that. One.

5 Q. Do you see that?

6 A. Yes.

7 Q. You told them that, right?

8 A. Yes.

9 Q. And then again in that interview, they covered with you
10 this issue of the screenshot that Mr. Kamaraju showed you on
11 direct, correct?

12 A. At some meeting I remember them discussing the screenshot.

13 Q. All right. I'm going to try and heed the admonishment and
14 not read from the document, so you read and see if that
15 refreshes your recollection.

16 A. Yes, I see it down here.

17 Q. OK. So they talked to you about this screenshot, correct?

18 A. Correct.

19 Q. And they asked you a lot of questions about it, correct?

20 A. Yes.

21 Q. They asked you when you had taken that screenshot, correct?

22 A. I don't remember the specific question, but I'm sure they
23 did.

24 Q. OK. And how many screenshots do you recall them showing
25 you?

K2dWsch2

Michael

1 A. I think three.

2 MS. SHROFF: OK. Can we just pull them up, please.
3 155.

4 Q. OK. So these are the three screenshots they showed you,
5 correct?

6 A. I counted this as one screenshot.

7 Q. Oh, OK.

8 A. In addition to the ones you just showed me earlier.

9 Q. OK. So take a look at the one farthest to the left.

10 A. OK.

11 Q. They asked you about this screen, correct?

12 A. Yes.

13 Q. They asked when you had -- you took -- I just want to make
14 sure.

15 You took a screenshot, correct? That means, like -- how
16 did you take it, by the way?

17 A. On the Windows operating system, on the keyboard, there's a
18 print-screen button. If you press that, it automatically puts
19 an image on your clipboard of what's on your desktop.

20 Q. And you did that, right?

21 A. Yes.

22 Q. And you did that on April 20?

23 A. Yes.

24 Q. And you, by the way, did not tell anyone about this,
25 correct?

K2dWsch2

Michael

1 A. Correct.

2 Q. But you told the FBI about it, or the FBI told you about
3 it?

4 A. The FBI showed me this screenshot and then asked me if I
5 had taken this.

6 Q. Is it fair to say, sir, by the time the FBI showed it to
7 you, you had forgotten about the screenshot?

8 A. Yes.

9 Q. You had taken it on April 20, 2016, right?

10 A. Yes.

11 Q. You forgot all about it?

12 A. Yes.

13 Q. You didn't talk to Mr. Weber about it, correct?

14 A. No.

15 Q. You didn't talk to Mr. Schulte about it, correct?

16 A. No.

17 Q. You didn't talk to anybody about it, correct?

18 A. Correct.

19 Q. And then the FBI started to ask you questions about this
20 screenshot, correct?

21 A. Yes.

22 Q. They asked you why you didn't tell anybody about it,
23 correct?

24 A. Yes.

25 Q. And they asked you what else or what all you did with the

K2dWsch2

Michael

1 screenshot, correct?

2 A. I remember questions about this screenshot. I don't
3 remember specifically what I did with it and stuff.

4 MS. SHROFF: OK. And can you move to the second page,
5 the second part of your --

6 Q. You're saying this is one, right?

7 A. This is one screenshot. I had three monitors, so when you
8 hit the print screen, it just takes all of those monitors and
9 puts it together as one screenshot.

10 Q. Oh, OK. So what does this have to do with anything? What
11 is the second page?

12 A. What this has to do with anything?

13 Q. Uh-huh.

14 A. I believe I was trying to dig into what the screenshot
15 meant. I was unsure. You know, I took the screenshot because
16 I was concerned, and then I tried to validate those concerns by
17 determining did a person do these reverts, or was this a system
18 action? This is me trying to dig into that. I have debug view
19 open to see if there was any debug messages about reverting the
20 VMs or something.

21 That could have been there already. I don't know. But
22 specifically this command prompt here that you see, this
23 black-and-white text, the command prompt, I was looking at IP
24 addresses.

25 Q. And did you do that on the same day, or you did this later?

K2dWsch2

Michael

1 A. No. Same day.

2 MS. SHROFF: OK. And let's move to the third part.

3 Q. This is also what you took, right? This is your third of
4 your three screens, right?

5 A. This is the right side, yes, of my screenshot.

6 Q. So you didn't tell anybody about any of these three shots,
7 correct?

8 A. Correct.

9 MS. SHROFF: Can I go back to the first one, please.

10 Q. Now, you see all the way at the bottom, this is on a
11 vSphere, correct?

12 A. Yes.

13 Q. Were you running the vSphere the whole day of April 20, or
14 you don't recall anymore?

15 A. It was very typical for us to just have this thing open for
16 days.

17 Q. For days, right?

18 A. Yes.

19 Q. So is it your testimony that -- you see the timing at the
20 bottom?

21 A. Yes. The start time?

22 Q. Yeah.

23 A. Yes.

24 Q. And you don't see anything before the start time of 6:55?

25 A. Yeah. I don't see anything before 6:55 -- or I see 6:51.

K2dWsch2

Michael

1 Q. Right, but you're saying that even though your vSphere was
2 running, you didn't see any April 16 snapshot?

3 A. Yeah. I don't see an April 16 snapshot.

4 Q. And sitting here, you don't remember seeing an April 16
5 snapshot, right?

6 A. Correct.

7 Q. Sitting here today, you don't remember how long this thing
8 had been running; it could have been running all day, and
9 that's common you already said, correct?

10 A. Correct.

11 Q. How many other people are running vSphere?

12 A. It was a common tool for the team to use.

13 MS. SHROFF: OK. You can take that down.

14 Q. Now, you said that it's common for people to remain logged
15 in to vSphere, correct?

16 A. Yes.

17 Q. Is it also common for people to remain logged in to DevLAN?

18 A. Yes.

19 Q. Is it common for people to stay logged in to the Same Time
20 chat thing?

21 A. No.

22 Q. OK. It's not common?

23 A. No.

24 Q. You log out of that one, right?

25 A. Same Time?

K2dWsch2

Michael

1 Q. Yes.

2 A. Yes, we log out of that one.

3 Q. Now, the screenshot that Mr. Kamaraju showed you and the
4 FBI showed you back then, you didn't talk about it with
5 Mr. Schulte?

6 A. Correct.

7 Q. You certainly didn't talk about it with Mr. Weber?

8 A. Correct.

9 Q. How about Karen?

10 A. No.

11 Q. Now, the FBI asked you repeatedly if you'd ever seen
12 Mr. Schulte carry hardware in or out of the CIA facilities,
13 correct?

14 Take a look at page 4. If you don't remember, take a look.
15 If you remember, just answer, please.

16 A. I don't remember the specific question. I'm looking for it
17 in the document.

18 Q. OK. Well, let's just start this way. You had never seen
19 him walking in and out with hard drives, correct?

20 A. Correct.

21 Q. And do you remember them asking you if Mr. Schulte ever
22 used something called a throwaway email account?

23 A. I don't remember the specific question.

24 Q. OK. Well, if they did ask you that question, would you
25 have said you do not recall him ever using any throwaway email

K2dWsch2

Michael

1 accounts?

2 A. I -- if I would have said that, I would change my opinion.

3 Q. OK. You would change your opinion now --

4 A. Yes.

5 Q. -- you're saying?

6 A. Yeah.

7 Q. But did you know him to use any throwaway email accounts?

8 A. It was common if we needed to register for, like, a free
9 site to use a throwaway email.

10 Q. What is a free site?

11 A. Like, if you need something online, like -- I'm having a
12 hard time thinking of something, but let's say I needed, like,
13 a code. Like, let's say there's a website that hosts code,
14 examples of code. Like, I want to copy this file, and this
15 website says, Hey, we have something that does that for you,
16 but you have to sign up for free to get that code sample. We
17 would use that throwaway account email to sign up to that
18 website and get the code sample, or do whatever it was.

19 Q. It's kind of like when you want to get something free and
20 you sign up --

21 A. Right.

22 Q. -- with an account, but you don't want to get those, Hey
23 come shop with us more?

24 A. Right, right, right.

25 Q. That's called a throwaway account?

K2dWsch2

Michael

1 A. Yes.

2 Q. That's a normal thing to do, right, in your business?

3 A. Yes.

4 Q. And everybody at the CIA had that type of CIA account?

5 A. I don't know about the whole CIA.

6 Q. And when I say the CIA, I just mean in your group.

7 A. Yes, certainly in my group that was a common thing.

8 Q. And you and he were in the same group, correct?

9 A. Yes.

10 Q. Do you recall them asking you if you ever used a spy pen?

11 A. I do not recall that.

12 Q. Now, is it in this interview, do you recall, if they asked
13 you if you would undergo a limited --

14 MR. KAMARAJU: Your Honor, could we have a sidebar?

15 THE COURT: Yes.

16 (Continued on next page)

K2dWsch2

Michael

1 (At sidebar)

2 MR. KAMARAJU: Thank you.

3 I believe where Ms. Shroff is about to go with this
4 question is to ask whether the FBI asked him to undertake a
5 polygraph exam. We have briefed extensively the idea of
6 polygraph exams being inadmissible. Your Honor ruled, in a
7 very narrow circumstance, some information about the
8 defendant's polygraph could come in, and the Second Circuit has
9 been very clear that polygraphs were exactly the purpose that
10 she's trying to introduce it -- sorry; I apologize -- that
11 polygraphs for the purpose of impeaching a witness are not
12 admissible.

13 THE COURT: Why did the government ask for it then?
14 Why did the government at the time ask for the polygraph?
15 Usually it's the defendant who says it's unreliable. Here,
16 it's the company, the CIA, or the FBI, that says it's
17 unreliable. Why isn't that the best of both worlds. You get
18 the polygraph and you get it accepted or rejected depending
19 upon the results. I don't understand the objection. I don't
20 think it's well-taken.

21 MR. KAMARAJU: Your Honor, whether we asked for the
22 polygraph or the defendant asked for the polygraph, the
23 question is whether you're going to get into the reliability of
24 polygraph examination.

25 MS. SHROFF: Your Honor, I'm going to make it easy for

K2dWsch2

Michael

1 Mr. Kamaraju. I'm just going to point out that the FBI asked
2 him to take a polygraph and he said no. There's nothing about
3 reliability here anyway.

4 THE COURT: OK. That ends it. Thank you.

5 (Continued on next page)

K2dWsch2

Michael

1 (In open court)

2 THE COURT: All right. Ms. Shroff.

3 Q. They asked you to take a limited polygraph?

4 A. Yes, at some point they did.

5 Q. And you declined, correct?

6 A. Yes.

7 Q. OK. Let's turn to your April 28 -- you can put that
8 document aside.

9 You next met with them in April of 2018. OK?

10 A. OK.

11 Q. And again, they asked you a lot of questions that are
12 repetitious, so I won't repeat them here, but do you recall if
13 they repeatedly asked you about this League of Legends game?
14 Do you recall that, or no?

15 A. No.

16 Q. They asked you about your friendship, and you explained
17 your friendship with Mr. Schulte to the FBI, is that correct?

18 A. Yes.

19 Q. You explained that you went to lunch together, correct?

20 A. Yes.

21 Q. He had this weird habit of putting a potato in the
22 microwave and keeping you waiting before you went to the
23 cafeteria, correct?

24 A. I thought that was normal, but that is true.

25 THE COURT: There you go.

K2dWsch2

Michael

1 Q. You explained to them that you went to the gym with him,
2 correct?

3 A. Yes.

4 Q. And you explained to them the nature of the relationship,
5 that you were friends, correct?

6 A. Yes.

7 Q. And again, they focused on the fact that you and he -- or
8 at least he had initiated contact with you after the leaks,
9 correct?

10 A. That is correct.

11 Q. Right. And that he had also texted you as part of that,
12 correct?

13 A. Yes, he texted me.

14 Q. Right. And when he texted you, he used his own phone,
15 correct?

16 A. Yes.

17 Q. He didn't refer to himself as anybody but Josh Schulte,
18 right, or as Josh?

19 A. Yeah. He didn't -- I just knew it was him because his
20 phone number was saved in my phone.

21 Q. It's the same phone number from before, right?

22 A. Yes.

23 Q. OK. They again asked you to talk to them about projects
24 that were worked on on thumb drives outside of the office and
25 brought into the office. Did they ask you about that; do you

K2dWsch2

Michael

1 remember?

2 A. I vaguely remember a question about -- I don't remember the
3 whole thumb-drive thing but a question about projects worked on
4 outside of the office.

5 Q. And one such project was Project Whiz. Do you remember
6 that project?

7 A. No.

8 Q. OK. But it's fair to say that people worked on a part of
9 the project outside of the CIA facility and brought it into the
10 facility, correct?

11 A. What was the question? Is it common?

12 Q. Yeah. People do that, right? I mean, I don't know how
13 common, but do people do that?

14 A. It was done. I would not say it was common.

15 Q. OK. But it was done, right?

16 A. Yes.

17 Q. And you told the FBI that, right?

18 A. I don't remember.

19 Q. OK. Take a look, if you want, at 3550-17. But you also
20 did tell the FBI that it was a one-way street; people didn't
21 take any work they did at the CIA outside the CIA, correct?

22 A. Right, I remember saying that, yeah, if you're going to do
23 a project outside, it comes inside, and then that's it; it
24 stays here.

25 Q. This one is easy.

K2dWsch2

Michael

1 A. One paragraph.

2 Q. The last page, and the only question is, does that refresh
3 your recollection?

4 A. This doesn't mention the outside projects. It just --

5 Q. Take a look at the last line. No?

6 A. Yup, it is there. I'm sorry.

7 Q. OK. Does that refresh your recollection, the last line,
8 that you told the FBI that?

9 A. Yes.

10 Q. OK. Now, you're still fully employed at the CIA at that
11 time, right?

12 A. Yes.

13 Q. OK. And then the next meeting you have with the FBI is on
14 August 16, 2019; yes?

15 A. I don't remember the date.

16 Q. OK. And at this meeting, you have two prosecutors present
17 and an FBI agent present. Does that ring a bell for you?

18 A. Uh, I don't remember who -- I feel like my first meeting
19 where there were prosecutors, there was more than two, but I
20 don't know for sure.

21 Q. Well, is this the first time you've met Mr. Kamaraju, do
22 you think?

23 A. I don't remember the date I met him. At some point I do
24 meet him for the first time.

25 Q. OK. And do you recall that during this meeting they again

K2dWsch2

Michael

1 told you that you had to be truthful? Correct?

2 A. I don't remember. But I do remember at varying points they
3 told me I had to be truthful.

4 Q. Right. And in this one, they actually told you that you
5 could have an attorney present if you want, right?

6 A. I don't remember.

7 Q. OK. Let me see if I can give you -- I'm going to give you
8 a document that ends with 027640.

9 A. Thank you.

10 OK. I've read the bullet points.

11 THE COURT: What's the question, Ms. Shroff?

12 BY MS. SHROFF:

13 Q. So, this is the meeting at which you are advised, if you
14 want, you can have an attorney, correct?

15 A. Uh, yeah. I think from the get-go, from my very first
16 meeting, they told me, you know, you have a right to have an
17 attorney. I don't think this is the first time I'm hearing
18 this.

19 Q. OK. So this doesn't strike, this meeting doesn't stick out
20 in your mind as anything different from any other one?

21 A. No. It does.

22 Q. It does, right?

23 A. Yes.

24 Q. OK. We'll get to that in a minute.

25 And in this meeting, they explained to you, did they not,

K2dWsch2

Michael

1 the difference between being questioned by the Department of
2 Justice and being questioned by the CIA people, correct?

3 A. I don't remember, like, a lengthy distinction between the
4 two.

5 Q. OK. Do you remember them trying to explain to you that
6 lying to them was a crime?

7 A. I don't remember that, but I do remember them at some point
8 saying you have to be truthful, truthful to us; it's a crime
9 not to be.

10 Q. OK. And at this meeting, they started substantively
11 talking with you about the screenshot that you had taken,
12 correct?

13 A. Yes. I see these -- I see that in the bullet points.

14 Q. OK. And then they asked you again, or at least they
15 started discussing with you the fact that you had told them
16 that you didn't remember taking that screenshot, correct?

17 A. Correct.

18 Q. And you again emphasized to them that you just didn't
19 remember taking that screenshot, correct?

20 A. Correct.

21 Q. You just didn't remember taking it on April 20, right?

22 A. Right.

23 Q. And you told them that you hadn't talked to Mr. Weber about
24 that screenshot; you told them this again, correct?

25 A. Correct.

K2dWsch2

Michael

1 Q. And you told them, did you not, that one of the reasons you
2 didn't talk to Mr. Weber is because you had tried to talk to
3 Mr. Weber before but he had blown you off, correct?

4 A. Correct.

5 Q. You tried to explain that to the FBI and the prosecutors,
6 right?

7 A. Yeah. Specifically he said stay out of it.

8 Q. Right. He told you to stay out of it, right?

9 A. Yes.

10 Q. Mr. Weber did?

11 A. Yes.

12 Q. And you told them that you had -- I mean, I don't know if
13 you used the word "investigated" but that you had investigated
14 the snapshot, right?

15 A. Yes, I had looked into it.

16 Q. And that you had investigated to see if that account was
17 accessing or using or missing logs, correct? Do you see that?
18 Look at the last bullet. Just read that whole bullet.

19 A. "M. investigated the snapshot to see why" --

20 Q. Don't read from the document.

21 THE COURT: Don't read aloud. Just read it to
22 yourself.

23 THE WITNESS: Oh, I'm sorry.

24 BY MS. SHROFF:

25 Q. Just read it to yourself.

K2dWsch2

Michael

1 A. OK.

2 Q. Now, you'd already talked to them many times, correct?

3 A. Yes.

4 Q. OK. And you explained to them that you didn't see any
5 logs, and then you tried to explain to them why it was -- what
6 the reason was why you may not see logs and that could be
7 logical, correct?

8 A. Yes. There could have been a good reason why that account
9 could not see the logs.

10 Q. Right. And that's because you had one kind of account, and
11 another kind of account would be needed to see the logs?

12 A. Yes, there's potential that the server was set up in such a
13 way where limited -- user accounts could not see the logs
14 whereas a full administrator account could.

15 Q. Right. And you explained that to them, right?

16 A. Yes.

17 Q. And then you told them that you were not sure that it was
18 Mr. Schulte who had done the reversions on April 20, correct?

19 A. Correct.

20 Q. And after you said that, they stopped the interview,
21 correct?

22 A. At some point they stopped the interview, yes.

23 Q. Right. And then you asked for a lawyer, correct?

24 A. I believe I asked for a lawyer before they stopped the
25 interview.

K2dWsch2

Michael

1 Q. Fair enough. You asked for a lawyer and they stopped the
2 interview, correct?

3 A. Yes.

4 Q. And at that time when you told them that you did not
5 believe that Mr. Schulte had done the reversion, you were still
6 a full-time employee at the CIA?

7 A. Correct.

8 Q. OK. And then that interview ended. By the way, where was
9 that interview?

10 A. Where was it?

11 Q. Yes.

12 A. It was here in New York.

13 Q. I'm sorry?

14 A. Here in New York.

15 Q. Oh, it was in New York?

16 A. Yes.

17 Q. OK. And the interview ended, right?

18 A. Yes.

19 Q. And then you left?

20 A. Yes.

21 Q. And did there come a time after the interview ended that
22 you went ahead and got yourself a lawyer?

23 A. Yes.

24 Q. And you hired a lawyer, Ed MacMahon, right?

25 A. Yes.

K2dWsch2

Michael

1 Q. Do I have his name right?

2 A. Yes.

3 Q. And the prosecutors had told you to have your lawyer call
4 them, correct?

5 A. Yes.

6 Q. And you had Mr. MacMahon -- you retained Mr. MacMahon,
7 correct?

8 A. Yes.

9 Q. He's a well-known criminal defense lawyer, correct?

10 A. Yes.

11 Q. Well-known for representing people who are accused of
12 wrongful conduct with leaks, right?

13 A. Yes.

14 Q. And you hired him and had him call them?

15 A. Yes.

16 Q. And right after this, is that when you learned that you
17 were put on administrative leave?

18 A. No. This was before, I, I -- so, right after the meeting,
19 I take a plane from New York back to Virginia, and I, you know,
20 sometime shortly after landing, I get a call from my division
21 chief.

22 Q. OK.

23 A. And my division chief said, Hey, come in through this
24 different entrance, and I -- I knew internally what that
25 probably what that meant. My division chief said he did not

K2dWsch2

Michael

1 know what that meant. So at that point I had a pretty good
2 idea that I was going to be -- something was going to -- some
3 sort of talking-to was going to happen.

4 Q. Right. But the talking-to had come after this meeting was
5 over, correct?

6 A. Correct.

7 Q. And the phone call you got from your division chief was
8 after this meeting was over?

9 A. Yes.

10 MS. SHROFF: Your Honor, would this be a good time to
11 take the morning break?

12 THE COURT: Yes, we'll take our morning break now.

13 (Continued on next page)
14
15
16
17
18
19
20
21
22
23
24
25

K2dWsch2

Michael

1 (Jury not present)

2 THE COURT: OK. You can stretch your legs.

3 THE WITNESS: Thank you.

4 (Witness not present)

5 THE COURT: Please be seated.

6 I'll see you in 15 minutes.

7 MS. SHROFF: Your Honor, I apologize. The document we
8 got this morning, I think we're only allowed to read it in the
9 SCIF, so I haven't seen it.

10 MR. KAMARAJU: We didn't say that, your Honor.

11 THE COURT: They didn't say that.

12 MS. SHROFF: Oh, it's marked classified, so I just
13 assumed it was the rule. Can I read it here?

14 THE COURT: You can read it here. It's in the
15 courtroom.

16 MS. SHROFF: Oh, OK. My bad.

17 (Recess)

18 (Pages 1321-1331 classified and sealed)

K2D3SCH3

(In open court; jury not present)

THE COURT: When I came down this morning, I directed the government produce the attachment to its letter of February 12. I did not direct that the letter itself from Mr. Kamaraju to me, from the government's team to me be produced, because I thought it had been produced. It lists on the cc list defense team by ECF and hand.

MR. KAMARAJU: I apologize.

THE COURT: That's all right. I subsequently directed that the letter be produced as well. And it has been produced now; is that correct?

MR. KAMARAJU: We're having a copy printed right now.

THE COURT: All right. Ms. Shroff, do you have an application? Mr. Zas.

MR. ZAS: Yes, your Honor. At this time, for the reasons we discussed in your Honor's chambers, the defense would move to suspend the examination of this witness and proceed to the next witness, recognizing that there is likely a need to recall this witness to complete both his cross-examination and his redirect examination.

THE COURT: All right. Mr. Kamaraju.

MR. KAMARAJU: We object, your Honor. We think that -- and we are obviously not privy to what defense counsel told you in the robing room. But to the extent --

THE COURT: Just as they were not privy to your

K2D3SCH3

1 memorandum and the letter that you transmitted the memorandum
2 with.

3 MR. KAMARAJU: Yes. We appreciate that, your Honor.
4 We're not objecting to fact that they spoke there, I'm just
5 caveating what I'm about to say.

6 To the extent the argument that they wanted to make,
7 which originally that they articulated was that they want to
8 suggest that the CIA badgered this witness into changing his
9 testimony through putting him on administrative leave. I think
10 Ms. Shroff was about to get there. They have the memo, if they
11 think that advances their point.

12 THE COURT: You are repeating what you said in your
13 letter, that she's more than adequately prepared for any
14 cross-examination she wants to make.

15 But this letter discloses something I hadn't seen
16 before, that Mr. Michael might have been a systems
17 administrator. That's what the memo says.

18 MR. KAMARAJU: First of all, all of the information
19 about his privileges have been disclosed to the defense for
20 years, or months at least, your Honor.

21 THE COURT: That he is a systems administrator?

22 MR. KAMARAJU: Yes, your Honor. We produced all the
23 log files to his computer, too. And multiple 302s have said
24 it. That's not a new fact to the defense, your Honor. That's
25 not something that has changed all of a sudden. So, if that's

K2D3SCH3

1 the basis, then all of that information --

2 THE COURT: The basis is the late production of this
3 information. I believe it should have been turned over at or
4 about the time that the decision was made. And I think it was
5 not accurate and not correct for you to withhold that
6 information until the witness took the stand.

7 At any rate, I'm going to grant Mr. Zas's motion.
8 He's going to be continued, continuation of the examination of
9 Mr. Michael.

10 Do you have another witness available?

11 MR. KAMARAJU: Yes, your Honor.

12 THE COURT: Okay. We'll call the other witness.

13 MR. KAMARAJU: The government calls Michael Berger.

14 THE COURT: Okay.

15 (Continued on next page)

K2D3SCH3

Berger - Direct

1 (Jury present)

2 THE DEPUTY CLERK: Please state your name for the
3 record.

4 THE COURT: Just a minute. I apologize for the long
5 break, not that you're probably too concerned about it. But we
6 had some important legal issues to take up and we're going to
7 resume now with another witness.

8 THE DEPUTY CLERK: Please state your name for the
9 record.

10 THE WITNESS: Michael Berger.

11 (Witness sworn)

12 THE DEPUTY CLERK: Witness sworn.

13 THE COURT: Please sit down, Mr. Berger.

14 MICHAEL BERGER,

15 called as a witness by the Government,

16 having been duly sworn, testified as follows:

17 DIRECT EXAMINATION

18 BY MR. KAMARAJU:

19 Q. Good morning, sir.

20 A. Good morning.

21 Q. Are you employed?

22 A. Yes, I am.

23 Q. Where do you work?

24 A. I work for the FBI.

25 Q. What's your position with the FBI?

K2D3SCH3

Berger - Direct

1 A. I'm a computer scientist.

2 Q. How long have you been a computer scientist with the FBI?

3 A. Approximately seven and a half years.

4 Q. Do you have any professional responsibilities in addition
5 to being a computer scientist with the FBI?

6 A. Yes, I do.

7 Q. What are those?

8 A. I also teach.

9 Q. Where do you teach?

10 A. I teach at the School of Engineering at New York
11 University.

12 Q. What do you teach?

13 A. I teach digital forensics.

14 Q. What's digital forensics?

15 A. Digital forensics is the concept of applying forensic
16 science principles to investigating digital evidence.

17 Q. How long have you been an adjunct professor?

18 A. About a year.

19 Q. I'd like to talk about your education for a second. Do you
20 have any undergraduate degrees?

21 A. Yes, I do.

22 Q. What was your undergraduate degree in?

23 A. It was a bachelor of science in computer science.

24 Q. How about graduate degrees?

25 A. I have a master of science in computer forensics, and a

K2D3SCH3

Berger - Direct

1 master of science in computer science.

2 Q. You mentioned computer forensics. What's that?

3 A. It's another word for digital forensics. It is the concept
4 of applying forensic science to investigating digital evidence.

5 Q. Prior to your work as a FBI computer scientist, do you have
6 any other experience in the information technology industry?

7 A. Yes, I do.

8 Q. Could you summarize that for us, please.

9 A. Before I worked for the FBI, I worked for a litigation
10 company as a digital forensics analyst.

11 Q. How long did you do that for?

12 A. About two years.

13 Q. When did you become an FBI forensic scientist -- excuse
14 me -- computer scientist?

15 A. I was hired in September of 2012.

16 Q. Generally speaking, what are your responsibilities as a FBI
17 computer scientist?

18 A. So, I work on a squad that investigates cyber intrusions.
19 And my job is to work with the agents and analysts on that
20 squad and provide subject matter expertise and perform
21 technical analysis when needed.

22 Q. When you say cyber intrusions, what does that mean?

23 A. It's a fancy way of saying hacking.

24 Q. You mentioned some technical work that you do.

25 A. Yes.

K2D3SCH3

Berger - Direct

1 Q. Can you tell us what you mean.

2 A. So, it is a wide range of tasks. Forensic analysis of
3 computers, analyzing captured memory, reviewing log files,
4 reverse engineering malware, also consult with agents prior to
5 them interviewing witnesses, sitting in on interviews, things
6 like that.

7 Q. Sir, are you familiar with the FBI CAT team?

8 A. Yes.

9 Q. C-A-T. What does CAT stand for?

10 A. That's the Cyber Action Team.

11 Q. What does the CAT team do?

12 A. The CAT team is managed out of our cyber division at
13 headquarters. It is the FBI's incident response team for cyber
14 incidents.

15 Q. When you say incident response team, what do you mean by
16 that?

17 A. Incident response is the process of responding to an
18 incident. So if an intrusion, a computer intrusion were to
19 occur at a institution, and they reached out and called the
20 FBI, depending on the scale of that intrusion, they might
21 deploy the CAT team to that incident.

22 Q. How are you familiar with the CAT team?

23 A. I'm a member of the team.

24 Q. How do you become a member of the CAT team?

25 A. There is a three-part application process.

K2D3SCH3

Berger - Direct

1 Q. Could you generally describe it.

2 A. The first part is a written application where you document
3 your experience and education in the field. If you -- they
4 accept your application, the next part is a practical. So it's
5 approximately four days where they give you evidence, they give
6 you limited information about a scenario. And you have to then
7 analyze that evidence, and determine what happened.

8 The third part of the process, if you pass the second
9 part, is a presentation. You then give a presentation --
10 almost like a mock presentation where you're presenting to both
11 people that are technical and non-technical, and you have to
12 explain what happened during this incident.

13 Q. Could you tell us what kind of investigations you've
14 participated in as a member of the CAT team?

15 A. A wide range of computer intrusions, hacking intrusions,
16 both nation state and criminal hacking.

17 Q. Just remind us, what is a nation state?

18 A. Nation state refers to hacking on behalf of either directly
19 from or on behalf of a foreign government.

20 Q. Have you participated in trainings related to your work?

21 A. Yes, I have.

22 Q. What kinds of training have you taken?

23 A. I've taken numerous trainings related to forensics and
24 other fields with information security.

25 Q. Have you received any kinds of certifications?

K2D3SCH3

Berger - Direct

1 A. Yes, I have.

2 Q. What certifications do you hold?

3 A. Directly relating to forensics, I hold the GIAC, which is
4 an organization, the certified forensic examiner as well as the
5 certified forensic analyst, as well as several other
6 certifications not directly related to forensics, but related
7 to information security.

8 Q. Generally speaking, what kind of certifications are the
9 information security certifications?

10 A. Certifications regarding just general information security,
11 network traffic analysis, security in regards to special
12 systems such as industrial control systems, things like that.

13 Q. In addition to the class you mentioned, have you ever done
14 any other kind of presentations?

15 A. Yes, I've done internal trainings at the FBI.

16 Q. Anything outside the FBI?

17 A. Just the teaching I believe.

18 MR. KAMARAJU: The government would offer Mr. Berger
19 as a expert in forensic computing, digital forensics, and
20 computer science.

21 THE COURT: Any objection?

22 MR. BRANDEN: May I ask a couple questions?

23 THE COURT: Yes, you may.

24 BY MR. BRANDEN:

25 Q. Mr. Berger, have you ever testified in court before?

K2D3SCH3

Berger - Direct

1 A. No, I have not.

2 Q. So you've never been approved as an expert before in the
3 field that you're purporting to be an expert in today?

4 A. Not in court, no.

5 MR. BRANDEN: I have no objection, Judge.

6 THE COURT: Okay. He's recognized as an expert.

7 MR. KAMARAJU: Thank you, your Honor.

8 Before we proceed, we have a stipulation that we'd
9 like to read into the record.

10 THE COURT: Yes, please.

11 MR. KAMARAJU: Ms. Hurst, can you pull up for just the
12 parties and the Court and the witness Government Exhibit 3002,
13 and just flip to the last page.

14 Paragraph 6 of the stipulation reads: It is further
15 stipulated and agreed that this stipulation, as Government
16 Exhibit 3002, and Government Exhibits 13501 through 1305-10 --

17 MR. BRANDEN: I think you said that incorrectly.

18 MR. KAMARAJU: Thank you.

19 1305-1, through 1305-10, Government Exhibit 1306-1,
20 Government Exhibit 1301-1 through 1301-4B, Government Exhibit
21 1302-1, and Government Exhibits 1304-1 through 1304-3, may be
22 received in evidence as Government Exhibits at trial.

23 And your Honor, we would offer the stipulation into
24 evidence as well as all the exhibits referred to there.

25 THE COURT: Any objection?

K2D3SCH3

Berger - Direct

1 MR. BRANDEN: No.

2 THE COURT: 3002 and all the exhibits referred to are
3 received in evidence.

4 (Government's Exhibit 3002, 1305-1 through 1305-10
5 received in evidence)

6 (Government's Exhibit 1306-1, 1301-1 through 1301-4B,
7 1302-1 received in evidence)

8 (Government's Exhibit 1304-1 through 1304-3 received
9 in evidence)

10 MR. KAMARAJU: If we can now publish the stipulation
11 for the jury. If we can go to the first page. At the moment
12 I'm just going to read the first two paragraphs.

13 If called as a witness, a representative of Google,
14 Inc. (Google) with knowledge of the matter would testify that
15 Government Exhibits 1305-1 through 1305-10 are true and correct
16 copies of documents from the account joshschultel@gmail.com,
17 including subscriber information, e-mails, and Google searches
18 conducted and websites visited by the user of that account, and
19 the date and times those searches occurred and the websites
20 visited search history, were made at or near the time by, or
21 from information transmitted by, a person with knowledge of the
22 matters set forth in the records; they were kept in the course
23 of a regularly conducted business activity; and it was the
24 regular practice of that business activity to maintain the
25 records.

K2D3SCH3

Berger - Direct

1 2. If called as a witness, a representative of
2 Amazon.Com, Inc. (Amazon) with knowledge of the matter would
3 testify that Government Exhibit 1306-1 contains true and
4 correct copies of documents from Amazon associated with Amazon
5 user account joshschultel@gmail.com, which were made at or near
6 the time by, or from information transmitted by, a person with
7 knowledge of the matters set forth in the records; they were
8 kept in the course of a regularly conducted business activity;
9 and it was the regular practice of that business activity to
10 maintain the records.

11 Now can we show for just the parties, the Court, and
12 the witness Government Exhibit 1704.

13 Q. Mr. Berger, can you take a look at what's on the screen.

14 A. Okay.

15 Q. Do you recognize it?

16 A. Yes, I do.

17 Q. How do you recognize it?

18 A. There's slides I've prepared.

19 Q. Were they prepared in connection with your testimony today?

20 A. Yes, they were.

21 Q. They represent a summary of your testimony today?

22 A. Yes, they do.

23 Q. Do they summarize exhibits you reviewed?

24 A. Yes.

25 Q. Will it aid in your testimony today, Government Exhibit

K2D3SCH3

Berger - Direct

1 1704?

2 A. Yes, it will.

3 MR. KAMARAJU: Your Honor, the government would offer
4 Government Exhibit 1704 as a demonstrative.

5 MR. BRANDEN: No objection.

6 THE COURT: It's received in evidence.

7 (Government's Exhibit 1704 received in evidence)

8 MR. KAMARAJU: If we can pull that up for the jurors,
9 please.

10 Q. Did there come a time when you became involved in an
11 investigation into something called Vault 7?

12 A. Yes.

13 Q. When did you start working on the Vault 7 investigation?

14 A. That was approximately the middle of March, 2017.

15 Q. Were you present in court for the testimony of Jeremy
16 Weber?

17 A. Yes, I was.

18 Q. Were you present for the testimony of Anthony Leonis?

19 A. Yes, I was.

20 Q. Did you hear them testify about the defendant's
21 administrative privileges with respect to a EDG project called
22 OSB libraries?

23 A. Yes, I did.

24 Q. Were you asked to review any forensic evidence relating to
25 changes in the defendant's administrative privileges in OSB

K2D3SCH3

Berger - Direct

1 libraries?

2 A. Yes, I was.

3 Q. Does this section of your presentation deal with that
4 analysis?

5 A. Yes.

6 Q. Go to the next slide, please.

7 So Mr. Berger, it is a little blurry. Can you explain
8 what we are looking at here?

9 A. So what we're looking at here is a query or a search done
10 on a restored version of the database. This particular
11 database was the Stash database that was saved on 4/16/2016. I
12 was able to restore that database into an active database, and
13 then search the data.

14 Q. If we can, what were you searching data for?

15 A. So this search was looking for activity between April 4,
16 2016, and the end of the database, so April 16. And it was
17 specifically looking for activity referencing the user Schuljo.

18 MR. KAMARAJU: So can we just focus on the top two
19 rows if we can blow those up, Ms. Hurst. Thanks.

20 Q. Could you explain what activity is reflected here.

21 A. Sure. So this is the -- the activity reflected here is the
22 user Weber removing administrative access from the user Schuljo
23 on the project OSB libraries.

24 Q. What's the date and time of that action?

25 A. That's April 4, 2016, at 11:21 a.m.

K2D3SCH3

Berger - Direct

1 Q. If we can go to the next slide. Do you recall Government
2 Exhibit 1061?

3 A. Yes.

4 Q. Who sent this e-mail?

5 A. This e-mail was sent from Josh Schulte.

6 Q. What is the date and time he sent it?

7 A. This was sent on April 14, 2016, at 3:39 p.m.

8 Q. If we go to the next slide. Do you see in this e-mail
9 where the defendant asked to be allowed to administer OSB
10 libraries?

11 A. Yes.

12 Q. In particular, do you see where he says, "I'd like to stay
13 on along with Frank Stedman and Jeremy Weber as helping
14 administrating them"?

15 A. Yes.

16 Q. Could you read the last line.

17 A. "So, if OSB and RDB would be okay with this, I would like
18 to continue my active role with the libraries."

19 Q. Can we take a look at the next slide, please. What's this?

20 A. This is an e-mail that was sent from Anthony Leonis.

21 Q. Who is it sent to?

22 A. Sent to Josh Schulte, Jeremy Weber, JoJo, Frank, and
23 Matthew. And it was cc'd to Sean, Richard, Frank Stedman, and
24 Kevin.

25 Q. When was this e-mail sent?

K2D3SCH3

Berger - Direct

1 A. This was sent on April 14, 2016 at 3:59 p.m.

2 Q. Do you recall Mr. Leonis testifying about this e-mail?

3 A. Yes, I do.

4 Q. Can we go to the next slide, please. Did Mr. Leonis
5 authorize the defendant at that time to act as an administrator
6 for OSB libraries?

7 A. No.

8 Q. Can we go to the next slide, please. We've looked at this
9 before; is that right?

10 A. Yes.

11 Q. Can we focus on the last two entries. What are we looking
12 at here?

13 A. So this represents the user Schuljo taking action to
14 reinstate admin privileges on the project OSB libraries for the
15 user Schuljo.

16 Q. When did he do that?

17 A. That was on April 14, 2016, at 4:05 p.m.

18 Q. When did this happen in relation to the e-mail from
19 Mr. Leonis that we just saw?

20 A. It was about six minutes after.

21 Q. So let's go to the next slide and just recap.

22 Can you just walk us through the timeline here.

23 A. Sure. So the timeline references how on April 4, Mr. Weber
24 removed the defendant's privileges to the OSB libraries, the
25 admin privileges to the OSB libraries. On April 14, at 3:39,

K2D3SCH3

Berger - Direct

1 the defendant requested his admin privileges be reinstated.
2 3:59 p.m., an e-mail response was sent saying the admin
3 privileges would not be reinstated. And at 4:05 p.m. the
4 defendant reinstated his own admin privileges.

5 Q. In addition to Mr. Leonis and Mr. Weber, were you also
6 present during David's testimony?

7 A. Yes.

8 Q. Did you hear all three of them testify about certain
9 actions on DevLAN on April 16, 2016?

10 A. Yes.

11 Q. What's your understanding of what those actions were?

12 A. My understanding is there were actions taken to lock down
13 or harden the system.

14 Q. Were you asked to review any forensic evidence in
15 connection with those actions?

16 A. Yes, I was.

17 Q. Can we go to the next slide, please. Could you explain
18 what we're looking at here?

19 A. So these are two different search results on the same
20 search, on the data from two different backups. So the first
21 screenshot is from the Crowd database from April 15, 2016. The
22 second screenshot is from the Crowd database on April 17, 2016.
23 So, before and after April 16.

24 Q. What's reflected here?

25 A. So this was a search for -- to reflect all the group

K2D3SCH3

Berger - Direct

1 memberships that user Schuljo was a member of.

2 Q. How do they change between April 15, 2016 and April 17,
3 2016?

4 A. On April 15, the user account was a member of the Atlassian
5 administrators group. By April 17, he was no longer a member
6 of that group.

7 Q. Can we go to the next slide. Was the defendant's
8 privileges the only ones that were changed on April 16, 2016?

9 A. No.

10 Q. What's reflected on this slide?

11 A. So this is similar in that the first screenshot reflects
12 the -- the Crowd database from April 15. And the second from
13 April 17. The search on the first screenshot is reflective of
14 all users that were member of a group with the word
15 "administrator" in them. And the same for the second
16 screenshot.

17 Q. How did it change?

18 A. So, there were several users that belonged to several
19 different types of administrator groups on April 15. By
20 April 17, there was only two accounts on the system that
21 belonged to groups that had the word "administrator" in them.

22 Q. Sir, were you present -- excuse me. Sorry.

23 Was the defendant continued to be listed there?

24 A. No.

25 Q. How about Jeremy Weber?

K2D3SCH3

Berger - Direct

1 A. No.

2 Q. How about Frank Stedman?

3 A. No.

4 Q. Sir, were you present for the testimony of Patrick Leedom?

5 A. Yes, I was.

6 Q. Did you hear Mr. Leedom testify about certain actions the
7 defendant performed on DevLAN on April 20, 2016?

8 A. Yes.

9 Q. Generally speaking, what's your understanding of what the
10 defendant did on that day?

11 A. My understanding is that on April 20, the defendant
12 performed a snapshot reversion on the OSB ESXi server reverting
13 the Confluence VM to a point in time when he was still part of
14 the administrator group.

15 Q. Did you hear Mr. Leedom testify about what happened during
16 that reversion?

17 A. Yes.

18 Q. What's your understanding of what happened?

19 A. In terms of?

20 Q. If any actions were taken.

21 A. There was activity shown on the system, there were --
22 evidence of log files being deleted. There is other activity
23 that was being presented -- that was happening during that time
24 frame coming from the defendant's DevLAN workstation.

25 Q. Did you hear Mr. Leedom testify about a March 3, 2016

K2D3SCH3

Berger - Direct

1 backup file?

2 A. Yes.

3 Q. What's your understanding of the significance of that file?

4 A. That the March 3 backup -- Mr. Leedom testified that the
5 March 3 backup file in his opinion was taken during that time.

6 Q. Were you asked to conduct any analysis of the EDG
7 information disclosed by WikiLeaks?

8 A. Yes, I was.

9 Q. Have you formed any opinions with respect to that
10 information?

11 A. Yes, I have.

12 Q. What opinions have you formed?

13 A. I was asked to perform analysis and conduct a timing
14 analysis and look at the data that was on WikiLeaks.

15 My opinion of that analysis is that the data that was
16 released on WikiLeaks came from a date range between March 2
17 and March 3, 2016.

18 Q. Was there a backup in existence on the Confluence -- was
19 there a Confluence backup file in existence on DevLAN within
20 that time range?

21 A. Yes.

22 Q. Which one was that?

23 A. It was the March 3 backup.

24 Q. So, if we go to the next slide and move on to the next one
25 after that. I'd like to start with how you arrived at that

K2D3SCH3

Berger - Direct

1 opinion. Could you describe your methodology, please.

2 A. Sure. So, I was asked to look at the data that was on
3 WikiLeaks and determine when it came from in the Confluence
4 system. In order to do that, we looked at the concept of
5 version control, which both Stash and Confluence employ.
6 Version control is a basic ability where you can make up dates
7 to documents or source code. And when you save them, they
8 don't completely overwrite your previous versions. The system
9 keeps track of the history of versions so it goes from version
10 1, version 2.

11 Q. Could you just get a little closer to the mic?

12 A. Sorry.

13 THE COURT: And slow down, too.

14 THE WITNESS: Sorry.

15 Q. I'm sorry to interrupt.

16 A. That's okay. Because we knew that the version control
17 existed on those systems, we could look at activity that
18 happened on those systems and we could look at data that was
19 posted on WikiLeaks.

20 We then looked for examples of data points of data
21 that was saved in the system that was present on WikiLeaks.
22 And data that was saved in the system that was not present on
23 WikiLeaks.

24 Q. You mentioned version control. Could you explain what
25 you're talking about there.

K2D3SCH3

Berger - Direct

1 A. Sure. So the easiest way would be if you create a
2 Microsoft Word document on your computer and you save it, you
3 then open it, you want to make some changes to it. Instead of
4 saving over the original file, you might go to file save as and
5 save it as version 2. You make some changes later on, you go
6 to save as version 3. You could then go into the folder on
7 your computer and would you see three different versions of the
8 document that reflect how it was when you saved it at each of
9 those points in time.

10 MR. KAMARAJU: Can we go to the next slide.

11 Q. Did you analyze the Stash data that was released by
12 WikiLeaks?

13 A. Yes.

14 Q. Could you walk us through how version control worked with
15 respect to Stash.

16 A. So Stash employed a version control that's common in the
17 software development industry. Underneath Stash it runs what's
18 called GIT. The concept of GIT is when you update your
19 software, and you write some code and you want to save it into
20 the repository, you end up with what's called a commit. You
21 are committing your code into the system. The code is saved,
22 and a record of the date and time that you saved the code.

23 Q. So, let's walk through what you did. What was the first
24 step for your Stash analysis?

25 A. We looked at the data that was on WikiLeaks and we tried to

K2D3SCH3

Berger - Direct

1 identify documents that we would be able to identify commit
2 actions on within the database.

3 MR. KAMARAJU: Can we go to the next slide, please.

4 Q. Are you familiar with a file called marble.horig?

5 A. Horig.

6 Q. Did you find such a file in the WikiLeaks release?

7 A. Yes, I did.

8 Q. Why did you look at that file?

9 A. So that file was a source code file. What I mean by that
10 is source code is generally referred to as plain text. There
11 are other types of documents, like Word documents and PDFs that
12 have text and other information stored within them. We were
13 aware that some of the documents that were posted on WikiLeaks
14 were converted when they posted it. So, in other words, there
15 might have been a Microsoft Word document for a user manual.
16 WikiLeaks converted the document to PDF and posted that PDF.
17 Because of that conversion, we couldn't make an identical
18 match. With a plain text file, we found they had posted actual
19 source code files without -- or what appeared had not actually
20 been converted. They just took the file as is and posted it.

21 Q. What did you do with this marble file?

22 A. So we computed what's known as a hash.

23 Q. What's a hash?

24 A. So a hash is a way of taking data and generating a
25 fingerprint for that data. The way a hashing algorithm works

K2D3SCH3

Berger - Direct

1 is you feed data in or what's known as the input, and you get
2 an output. The output looks like that string that's on the
3 screen. Lots of letters and numbers.

4 The concept of hashing is that if you -- one of the
5 concepts -- if you always feed in the exact same input data,
6 you will always get the same hashing data. It's very useful in
7 forensics if you want to confirm that two files are identical.
8 If they look similar, you can then compute a hash on them, and
9 then you'll see that the hash matches, and you would know these
10 files are identical.

11 Q. Can we go to the next slide, please. Could you tell us
12 what we're looking at here.

13 A. So this is some data that we retrieved from the Stash
14 backup files. We looked at that particular file, marble.horig,
15 and we were able to see what's known as the commit history for
16 it.

17 Q. And there are a couple of things in the MD5 column that are
18 highlighted in blue here. Do you see that?

19 A. Yes.

20 Q. Why are they highlighted in blue?

21 A. Those indicate that they matched the hash computed from the
22 file as it appeared on WikiLeaks.

23 Q. Do you have an understanding of why there are two?

24 A. Yes. So, one possibility for it would be if someone saved
25 a commit on February 26 at 9:36 a.m., they then made a change

K2D3SCH3

Berger - Direct

1 one minute later at 9:37 a.m. It's possible that on March 1st,
2 they realized that they didn't want that change anymore or
3 maybe it was an inadvertent change and saved. They could have
4 rolled back to the data that was on February 26 at 9:36 and
5 recommitted that version.

6 Q. Can we look at the next slide, please. So, what are we
7 looking at on this timeline?

8 A. This is just another representation showing that the files
9 that we just looked at, and representing them across a
10 timeline. The data points that are beneath the timeline that
11 are in green, those are versions of the file that appeared on
12 WikiLeaks.

13 Q. Let's take a look at another file. Next slide, please.
14 What are we looking at here?

15 A. So, this another file that we identified referred to as
16 solution events or the file name was SolutionEvents.cs. As the
17 file appeared on WikiLeaks, we computed the hash value to be
18 what you see on the screen.

19 Q. Is this another source code?

20 A. That's another source code file or plain text.

21 Q. Can we move to the next slide. Could you explain what's
22 going on here?

23 A. Sure. So, similarly, we looked at the commit history for
24 this particular file as well. And we noticed that on
25 February 13, 2016, at 3:13 p.m., the file was committed and it

K2D3SCH3

Berger - Direct

1 was identical to the file as it appeared on WikiLeaks.

2 Q. Based on your analysis of the marble and solution events
3 file data, were you able to reach any conclusions?

4 A. Yes, I was.

5 Q. Can we go to the next slide, please. What conclusions were
6 those?

7 A. So looking at the data that was both present in the
8 database and present on WikiLeaks, and present in the database
9 and not present on the WikiLeaks, we were able to determine at
10 what point the data sort of stopped that WikiLeaks had.

11 Q. Let's take a look at the next slide. Is that represented
12 here?

13 A. Yes, it is.

14 Q. So what was your conclusion as to when the data, the range
15 for the data?

16 A. For Stash we identified the range of data being from
17 February 26, 2016, at 9:36 a.m., and March 4, 2016, at
18 9:45 a.m.

19 Q. Can you remind us, was there an identical hash for the
20 marble file at March 1st?

21 A. Yes, there was.

22 Q. Was there a reason why you didn't use March 1st here
23 instead of February 26?

24 A. Yes.

25 Q. What's that?

K2D3SCH3

Berger - Direct

1 A. The reason is because that the files were identical, we
2 didn't want to assume that the data had to have come after
3 March 1st. We took a more conservative approach and we slid
4 our date back to being as possibly coming from after
5 February 26 instead.

6 Q. We can move on to the next slide. Did you do a similar
7 analysis with respect to Confluence?

8 A. Yes.

9 Q. Take a look at the next one. What are we looking at on
10 this page?

11 A. So this is again another database search. What we're
12 looking at here is a Confluence database backup from April 25,
13 2016, and we're looking at a list of revisions for a particular
14 page.

15 Q. Okay. So let's just walk through this a little bit.

16 A. Sure.

17 Q. Let's start with the left the title content ID. What's
18 that column?

19 A. So every page, even every page revision in Confluence gets
20 its own unique content ID.

21 Q. And content type?

22 A. In this case they're all pages. There are other types of
23 content, such as if you make an attachment to a page, that
24 would be listed as its own unique entry in the database, and it
25 would be of type attachment.

K2D3SCH3

Berger - Direct

1 Q. And moving one more column to the right. What do we have
2 there?

3 A. So that is the title. The left and the title 16 were just
4 formatting, so the entire title would display in the window
5 here. That is the title of this particular page.

6 Q. And moving over to version. What's listed in version?

7 A. So that's the version of the page. So, as you would update
8 the page and new versions were created, it would keep track of
9 all the previous versions.

10 Q. How many versions are reflected here?

11 A. So this query lists 17 versions.

12 Q. Moving over to the next column. Creation date. What's
13 that?

14 A. So the creation date, as you can see is identical across
15 all versions. It seems to have stored the creation date of the
16 overall page, not each individual version of the page.

17 Q. Is there a column that shows when each version of the page
18 was created?

19 A. Yes. The last mod date, the next column.

20 Q. And what's the column, prev ver?

21 A. That's a unique value that's assigned within the database
22 for all the different versions of the same page.

23 Q. And page ID?

24 A. Not sure what the values that are null, what those
25 reference. There are other types of content in the database.

K2D3SCH3

Berger - Direct

1 Actually, I believe the page ID might reference for when
2 there's content that's not pages, how it links back to a
3 particular page.

4 Q. Can we go to the next slide, please. What's this?

5 A. This is a copy of one of the pages as it appeared on
6 WikiLeaks.

7 Q. Which page are we looking at?

8 A. So it's identified here as saying user number 3375130's
9 home. We identified this as being a version of the Michael R's
10 home page.

11 Q. How did you do that?

12 A. So we looked at the page. We looked at the content on the
13 page. We also looked what you're asking about in the previous
14 slide, that prev ver number that was a unique value across all
15 the different pages. You can see here that's actually part of
16 the name of the page as it was pushed out on WikiLeaks. It
17 says page_3375129.html.

18 Q. We just go back to the last slide. Can you point out where
19 that number appears.

20 A. Sure.

21 MR. KAMARAJU: Go forward again.

22 Q. Are you able to tell by looking at this page what version
23 of the page we're looking at?

24 A. Yes, so if you look at the bottom, you'll see how there are
25 included links to previous versions. And the numbers one

K2D3SCH3

Berger - Direct

1 through 16 are displayed. That indicated that this is the 17th
2 version of the page.

3 Q. Can we move on to the next slide, please. How many
4 versions of Michael R's home page are reflected here?

5 A. 17 versions listed.

6 Q. So, are we looking at the same number that existed on the
7 WikiLeaks page?

8 A. Yes.

9 Q. Can we have the next slide, please. What's this?

10 A. This is another page that came from the WikiLeaks release.

11 Q. What's the name of this page?

12 A. It's entitled Build Felix LP.

13 Q. How do you know that?

14 A. It's the appears in the title bar of the browser right
15 before it says Mozilla Firefox.

16 Q. You testified previously about a prev ver number; is that
17 right.

18 A. Yes.

19 Q. Is there a prev ver number for this one too?

20 A. There is a number that's reflected in the file name here
21 where it says page_52625416.html.

22 Q. Are you able to tell from looking at this page how many
23 versions of Build Felix LP this is?

24 A. So this page lists that there are seven previous versions,
25 indicating that this is the eighth version of the page.

K2D3SCH3

Berger - Direct

1 Q. Can we go on to the next slide. What are we looking at
2 here?

3 A. This is a query from the Confluence backup from April 25,
4 2016. Looking for all the pages that match that same prev ver,
5 the 52625416.

6 Q. Can you tell from this when the eighth version of the Build
7 Felix LP page was created?

8 A. Yes.

9 Q. When was that?

10 A. So I'm going to circle it right here. That was on March 2,
11 2016, at 8:01 a.m.

12 Q. I think you circled it there, too. When was the ninth
13 version created?

14 A. It's in the same circle. The ninth version was March 3,
15 2016, at 6:47 a.m.

16 Q. And the information that WikiLeaks disclosed, was that from
17 the eighth version or the ninth version?

18 A. That was from the eighth version.

19 MR. KAMARAJU: Can we move on to the next slide.

20 Q. So let's walk through this. What are we looking at here?
21 Let's start on the left.

22 A. So this illustrates how on March 2, 2016, at 8:01 a.m.,
23 Build Felix version 8 was saved in Confluence. And the page in
24 WikiLeaks shows seven previous versions.

25 Q. What do we know about the Michael R. home page version?

K2D3SCH3

Berger - Direct

1 A. So on March 2, 2016, at 3:58 p.m., Michael R's home version
2 17 was saved in Confluence. And the Michael R's home on
3 WikiLeaks shows 16 previous versions.

4 MR. KAMARAJU: Can we move on to the next slide.

5 Q. There a lot going on in this one. Let's take it slow.
6 Start on the one on the left. So what are we looking at there?

7 A. Starting again from the left, from the top left.

8 Q. Yes. The March 2, 2016, 8:01.

9 A. March 2, 2016, 8:01 a.m. Build Felix version 8 was saved in
10 Confluence, and the Build Felix page in WikiLeaks shows seven
11 previous version.

12 On March 2, 2016 at 3:58 p.m. Michael R's home page
13 version 17 was saved in the Confluence database, and the
14 Michael R's home on WikiLeaks shows 16 previous versions.

15 On March 3, 2016, at 6:47 p.m. Build Felix version 9
16 was saved in Confluence. This version is not reflected in the
17 data on WikiLeaks.

18 Q. Why is that significant?

19 A. It gives us an indication of where the boundary is of the
20 data that WikiLeaks does not have.

21 Q. So what conclusions were you able to draw?

22 A. That the data that WikiLeaks had was between those two
23 points.

24 Q. Let's move on to the next. What does this reflect?

25 A. This reflects both the Stash and Confluence analysis.

K2D3SCH3

Berger - Direct

1 Looking at Stash, we can see that the data that was on
2 WikiLeaks corresponds to the data from between February 26, at
3 9:36 a.m. and March 4, at 9:45 a.m.

4 Looking at the Confluence data points, we're able to
5 get a smaller window that shows between March 2, 3:58 p.m. and
6 March 3, at 6:47 a.m.

7 Q. So the band in blue there, what's that mean?

8 A. That is the band for the Confluence data points.

9 Q. Remind us, what are the end points for that?

10 A. March 2nd at 3:58 a.m. and March 3 at 6:47 a.m.

11 Q. Can we take a look at the next slide. Do you recognize
12 what we're looking at here?

13 A. Yes, I do.

14 Q. What is it?

15 A. These are directory listings of Confluence backup files.

16 Q. Do you remember Mr. Leedom testifying about these?

17 A. Yes.

18 Q. I'd like to go to the next slide. Do you see any backup
19 files that fit the criteria that you addressed earlier?

20 A. Yes, I do.

21 Q. Which one is that?

22 A. That is the Confluence backup file from March 3.

23 Q. Why does it fit your criteria?

24 A. That file was created on March 3, at 6:25 a.m. and finished
25 completion at 6:29 a.m. That backup file, when it was

K2D3SCH3

Berger - Direct

1 generated, fits within that window.

2 Q. You said 6:25 a.m. Do you see the date modified column?

3 A. Yes.

4 Q. What's the date modified column listed there?

5 A. 6:29 a.m.

6 Q. What's the difference?

7 A. That's just an indication of when the backup process first
8 started creating the backup, and when it was finished writing
9 the data to the file.

10 Q. And with respect to the tgz files, do you see any of those
11 that match your criteria?

12 A. Yes.

13 Q. Which one is that?

14 A. The March 3 file.

15 Q. When was that created?

16 A. That was created, it looks from the name of the file, it
17 was created initially at 6:25 and then finished saving at
18 6:29 a.m.

19 Q. Can we move to the next slide, please.

20 So, putting all this data together, what are we
21 looking at here?

22 A. So this reflects the timeline, the combined timeline from
23 the Stash and Confluence analysis. And it reflects how the
24 March 3 backup file fits into that window.

25 Q. Does it fit into the window you had previously identified

K2D3SCH3

Berger - Direct

1 with the blue band?

2 A. Yes.

3 Q. Let's move to the next slide, please. We just looked at
4 this. What's the date accessed for the March 3 backup file?

5 A. The date accessed for the March 3 SQL file is 5:42 p.m. on
6 April 20.

7 Q. What year?

8 A. Of 2016.

9 Q. How about that tgz file?

10 A. The date accessed for March 3 tgz file was April 20, 2016,
11 at 5:43 p.m.

12 Q. We can go to the next slide. In addition to the work that
13 you did on DevLAN, did you take at any of the defendant's home
14 media?

15 A. Yes, I did.

16 Q. Could you describe generally how he had his home computer
17 network set up?

18 A. Sure. So he had a desktop computer that consisted of four
19 hard drives. There was a single hard drive that operated as
20 the system drive, or in Windows referred to it as the C drive,
21 and there were three additional hard drives that combined to
22 form what's known as a RAID volume.

23 Q. What's a RAID volume?

24 A. So a RAID volume is a way of combining multiple hard drives
25 and presenting to the user as a single large volume of data.

K2D3SCH3

Berger - Direct

1 It has redundancy built in depending on the configuration, so
2 if one those hard drives were to fail, you don't lose the data,
3 the data is still stored on the other two, and you can replace
4 that hard drive.

5 Q. Did you call it a RAID 5?

6 A. Yes.

7 Q. What's the five mean?

8 A. The RAID 5 is just a type of RAID configuration.

9 Q. You remember hearing earlier about virtual machines?

10 A. Yes.

11 Q. You remember hearing about how virtual machines can be
12 created on computers?

13 A. Yes.

14 Q. Are you familiar with virtual machines?

15 A. Yes, I am.

16 Q. What are virtual machines?

17 A. Virtual machine is a way of representing a computer inside
18 of a computer. It is a way that allows you to run different
19 operating system other than the primary operating system you'd
20 run on your main computer.

21 Q. Did the defendant run any virtual machines on his home
22 computer network?

23 A. Yes.

24 Q. Let's take a look at the next slide. What are we looking
25 at here?

K2D3SCH3

Berger - Direct

1 A. So this is the initial power on screen to a Linux virtual
2 machine that was present on the defendant's workstation.

3 Q. You see the bullets, dot dot dot dot dot?

4 A. Yes.

5 Q. What do those represent?

6 A. So when this virtual machine was powered on, it presented a
7 prompt, you enter a password. This screenshot represents after
8 you've typed that password, before you would hit the enter key,
9 it represents a password being entered.

10 Q. So let's look at what happens next. Can we go to the next
11 slide. What's this?

12 A. So after you have entered the correct boot password, the
13 virtual machine would start to boot up. Once it finished that
14 process, it would present you with the desktop and or a log on
15 screen to get to the desktop.

16 Q. Do you see a user name here?

17 A. Yes.

18 Q. Whose user name is here?

19 A. Josh.

20 Q. What did you do next?

21 A. If you enter the password for that user account, and then
22 click OK, you would be presented with the desktop for the
23 virtual machine.

24 Q. Let's take a look at the next slide. What's this?

25 A. This is the desktop of the virtual machine.

K2D3SCH3

Berger - Direct

1 Q. Just remind us, whose desktop?

2 A. This is the desk, the virtual machine that was on the
3 defendant's computer.

4 Q. Do you see it says Linux Mint there?

5 A. Yes.

6 Q. Do you know what that is?

7 A. So Linux Mint is a particular distribution of Linux.

8 Q. When you say distribution, I just -- what do you mean by
9 that?

10 A. So Linux itself is open source. The core part of the
11 operating system, different people, different organizations
12 will take that and package it in different ways, customize how
13 it looks with different utilities and they'll release different
14 distributions of Linux.

15 Q. On the left side there, starting with computer. What are
16 those icons?

17 A. Those are desktop icons.

18 Q. Are those icons the way it appears on the defendant's
19 virtual machine desktop?

20 A. Yes.

21 Q. Let's walk through. The green folder marked "home," what's
22 that?

23 A. That's the home folder for the user account that we're
24 logged into here. The home folder is similar to how your home
25 folder works on a Windows or Apple computer. Within there you

K2D3SCH3

Berger - Direct

1 might have folders for documents, pictures, videos, things like
2 that. It's where you put most of your user content for
3 yourself. Different -- each user account would have their own
4 home folder.

5 Q. The one below that, what's that?

6 A. That's an icon for the Tor browser.

7 Q. What does that icon represent?

8 A. So the Tor browser is a web browser that allows you to
9 connect to the Tor network.

10 Q. What's the Tor network?

11 A. The Tor network is a system of computers that are
12 connected, if you connect to it through a Tor browser, it
13 allows you to connect to websites in a way that those websites
14 are not able to trace where you're coming from.

15 Q. How does that work?

16 A. It essentially routes your traffic through a series of
17 encrypted tunnels through a series of different computers that
18 are running Tor software.

19 Q. When you're using Tor, are you able to see any different
20 websites?

21 A. Yes, you are.

22 Q. Could you explain that, please?

23 A. You're able to see what's referred to as a Tor hidden
24 service. That is a web server that is running specifically on
25 the Tor network. Whereas most websites you go to might end in

K2D3SCH3

Berger - Direct

1 dot com or dot net, a Tor hidden service would end in the dot
2 onion phrase. The unique feature of the Tor hidden service,
3 just as you are using the Tor browser, you're protecting where
4 no one can see where you're coming from. A Tor hidden service
5 is hiding where it's being hosted. So if an organization
6 wanted to set up a web server, and allow people to connect to
7 it but make it very difficult to determine its location, they
8 could run it as a Tor hidden service.

9 Q. Could you give us an example of a Tor hidden service?

10 A. I believe WikiLeaks has a link to a version of their site.
11 It ends at dot Onion.

12 Q. What's the icon below the Tor browser there?

13 A. That's for VeraCrypt.

14 Q. What's that?

15 A. VeraCrypt is an encryption program, it's used to encrypt
16 and decrypt data.

17 Q. What's encryption?

18 A. Encryption is a way of securing your data. Obfuscating it
19 so if you use a particular key or password to lock that data,
20 you're unable to get back in and see that data unless you have
21 the correct password.

22 Q. Generally speaking, how does VeraCrypt work?

23 A. So, there's two methods that are generally used. You can
24 either encrypt a hard drive completely, or you can create
25 what's known as an encrypted container. This would -- think of

K2D3SCH3

Berger - Direct

1 it as kind of like a zipped file, where it is a file where you
2 put other files. You create an encrypted container, you would
3 mount it and it appear as a window. You can then drag other
4 files into it. When you unmount that encrypted container, it
5 would go back to being a single file on your computer that is
6 encrypted. In order to then mount that file again and view its
7 contents, you would need the password or key for that file.

8 Q. Did you try to mount any encrypted containers?

9 A. Yes, I did.

10 Q. Let's walk through that process. Go to the next slide.
11 What are we looking at here?

12 A. So this a screenshot of when you open VeraCrypt, as
13 indicated here, I've selected a particular file here.

14 Q. That says slash home. What's that a reference to?

15 A. So on Linux, the slash home is where the user account
16 folders would go. So, under the slash home directory, you
17 would see a slash Josh directory. That would be indicative of
18 the home folder for the user account Josh.

19 Q. What's this file called?

20 A. This file is called data.bkp.

21 Q. Let's go to the next slide. What happens after you try to
22 mount it?

23 A. So when you click mount, you would be prompted to enter the
24 password for that container.

25 Q. Did you try to enter the password?

K2D3SCH3

Berger - Direct

1 A. Yes, that's represented by those black circles in the
2 password box.

3 Q. What happens after you enter the password?

4 A. After that, you would then click OK.

5 Q. Okay. Once you click OK, what happens?

6 A. Another prompt would come up, prompting for an
7 administrator password.

8 Q. What's an administrator password?

9 A. So, Linux, the administrator account is referred to as the
10 root account. This is prompting you for the administrator
11 password or the password of a user who has privileges to mount.
12 The reason being is that mounting, when you're -- when you're
13 decrypting an encrypted container, it's what's known as
14 mounting a file system. It's going to appear as a virtual
15 disc. That's how VeraCrypt connects the data to the system.
16 Mounting a file system in Linux requires root privileges.

17 Q. Do you know if the defendant ever tried to mount any
18 encrypted containers?

19 A. Yes.

20 Q. I'd like to direct your attention to April 18, 2016. Do
21 you know if he tried to mount any containers on that day?

22 A. Yes.

23 Q. Let's go to the next slide. How do you know?

24 A. You can see here, these are entries from a particular log
25 file referred to as auth.log.1. On April 18, you can see here

K2D3SCH3

Berger - Direct

1 particularly the entry.

2 Q. Let me ask you a question before you go on. What's auth.
3 log?

4 A. So the auth. log represents a log file on Linux where
5 authentication related activity is stored.

6 Q. What do you mean by authentication?

7 A. It would be like logging in with your password.

8 Q. So, now I believe you were about to talk about some
9 particular entries here.

10 A. Yes.

11 Q. Please describe those?

12 A. So you can see the two lines where I've circled the
13 beginning of the line, towards the end of that line where it
14 says command user bin VeraCrypt core service, then again on the
15 next line. This was indicative of trying to mount an encrypted
16 container with this particular version of VeraCrypt.

17 The reason that it says one incorrect password
18 attempt, what I mentioned before where you need root
19 privileges, when VeraCrypt tries to mount the container it
20 doesn't have root privileges. It then prompts you for an
21 administrator password, and will be able to mount the container
22 given an appropriate password.

23 Q. How do you know that's how VeraCrypt works?

24 A. Because I researched the product, researched this
25 particular message, and we recreated the steps of mounting it

K2D3SCH3

Berger - Direct

1 and verifying the contents of the log file.

2 Q. Do you know if the defendant actually accessed the
3 VeraCrypt container?

4 A. Yes.

5 Q. Go to the next slide, please. How do you know that?

6 A. So this file represents recently used activity. Several
7 versions of Linux have this file, it's kind of like a history
8 file for things you do on a file system. You can see here that
9 it references the file/home/josh/data.bkp. You can see the
10 application name referenced with that file was VeraCrypt.

11 Q. What's the date of this access attempt?

12 A. So the date on the access attempt, I'll circle it right
13 here. It's listed here as April 19, 2016, at 3:03 a.m.
14 However that is marked as Zulu time. So that would correspond
15 with 11:03 p.m. on April 18.

16 Q. That would be local time?

17 A. Yes.

18 Q. This is from April 18. Were you asked to look at any other
19 forensic evidence from April 2016 from the defendant's home
20 network?

21 A. Yes.

22 Q. Let's start with April 23, 24. You know what Tails is?

23 A. Yes, I do.

24 Q. Go to the next slide. Do you know what a SATA adapter is?

25 A. Yes, I do.

K2D3SCH3

Berger - Direct

1 Q. What are we looking at?

2 A. This is an order confirmation e-mail from Amazon sent to
3 Josh Schulte.

4 Q. And what's the date of it?

5 A. Sunday, April 24, 2016, at 12:39 a.m.

6 Q. What's the product that's referred to here?

7 A. The product listed is an Inatek USB 3.0 SATA.

8 Q. You see the name am is cut off there a little bit.

9 A. Yes.

10 Q. Let's go to the next slide and see if we can expand that.
11 What's this?

12 A. So these are the results of a search warrant to Amazon for
13 those order details.

14 Q. Do you see an item description?

15 A. Yes.

16 Q. Could you read that description.

17 A. Sure. Inatek USB 3.0 to SATA dual bay USB 3.0 hard drive
18 docking station with offline clone function for 2.5-inch and
19 3.5-inch HDD SSD SATA (SATA 1/2/3).

20 Q. Do you know what that is?

21 A. Yes.

22 Q. What is it?

23 A. So this is what's referred to as a docking station. It is
24 a small device that you would be able to hook up to your
25 computer and insert hard drives into it.

K2D3SCH3

Berger - Direct

1 Q. Do you see where it says shipped?

2 A. Yes.

3 Q. What's the shipped date listed there?

4 A. The ship date is listed as April 24, 2016.

5 Q. Is that the same date as we saw the order confirmation for?

6 A. Yes.

7 Q. Do you know if Amazon offers same day shipping?

8 A. I've heard that they do, yes.

9 Q. Do you see the ship method listed as lasership_INJ_same?

10 A. Yes.

11 MR. KAMARAJU: Can we go to the next slide, please.

12 Q. What are we looking at here?

13 A. So these are the results of a search warrant to Google for
14 searches from the defendant.

15 Q. Let's just start at the bottom one. What's the date and
16 time of that?

17 A. That is April 24, 2016, at 2:42 p.m. UTC which would be
18 10:42 a.m. local time.

19 Q. Is that after the order confirmation that we looked at from
20 before?

21 A. Yes.

22 Q. What did the defendant search for here?

23 A. He was searching for a SATA adapter.

24 Q. What's a SATA adapter?

25 A. A SATA adapter is something that allows you to connect a

K2D3SCH3

Berger - Direct

1 SATA interface on a hard drive and connect it to another type
2 of interface.

3 MR. KAMARAJU: Your Honor, may I approach?

4 THE COURT: Yes, you may.

5 Q. I'm showing what's been entered into evidence as Government
6 Exhibit 1603, 1609, and 1610.

7 Do you recognize Government Exhibits 1609 and 1610?

8 A. Yes.

9 Q. What are they? You can take them out of the bag, too.

10 A. 1609 and 1610, right?

11 Q. Yes.

12 A. They are both hard drives.

13 Q. I believe we saw a stipulation before that they were --
14 I'll put the stipulation in.

15 Now hard drives, could you take them out of the bag,
16 please.

17 A. Sure.

18 Q. Would that kind of hard drive work with the Inatek SATA
19 adapter?

20 A. Yes.

21 Q. Could you demonstrate for jury how that would work.

22 A. Sure. So, if you see on the side right here there is some
23 connections. These connections right here, there is a longer
24 connection and a shorter connection. The shorter connection,
25 longer connection are both the data channel and the power

K2D3SCH3

Berger - Direct

1 channel. The SATA adapter that was ordered, if you can picture
2 like a toaster with two slots on top of it. You would take the
3 hard drive, and you would, with those connections facing down,
4 drop it into one of the slots, it would meet receiving
5 connections on the inside of the device.

6 Q. Once you connect to the device, what would you be able to
7 do?

8 A. Once you connect to the hard drive into the device, the
9 device would have a power cord, you plug and give it power and
10 would have a USB cable coming out of it. You could then plug
11 that into your computer and you could read and write data from
12 the hard drive.

13 Q. Government Exhibit 1610.

14 A. Okay.

15 Q. Would that type of hard drive work with the SATA adapter?

16 A. Yes, it would.

17 Q. What's the size of Government Exhibit 1609 and Government
18 Exhibit 1610?

19 A. Each one is a one terabyte hard drive.

20 Q. Let's take a look back at the Google searches for a second.
21 Do you see a search on April 24, 2016, at 14:4:37 UTC?

22 A. Yes.

23 Q. Do you see where it says searched for SATA PCI card?

24 A. Yes.

25 Q. What's a SATA PCI card?

K2D3SCH3

Berger - Direct

1 A. A SATA PCI card is another way of connecting a SATA hard
2 drive to your computer. Whereas the docking station would
3 allow you to connect hard drives externally outside your
4 computer, a SATA PCI card would be a card you install inside
5 your computer. Most desktop computers have what we refer to as
6 expansion slots. These are empty slots that the manufacturer
7 gives you to add functionality later on. You would open up the
8 side panel of your computer and insert the PCI card. On the
9 card itself there would be additional ports to connect to a
10 SATA hard drive.

11 Q. Would that work the same way with respect to data transfer
12 as the SATA adapter?

13 A. Yes.

14 Q. So would you be able to transfer data to the hard drive
15 that you had connected?

16 A. Yes.

17 Q. Can we take a look at the next slide. What are we looking
18 at here?

19 A. This is a shipping confirmation e-mail from Amazon.

20 Q. If we just blow up the top there. What's the date and
21 time?

22 A. I believe that is Sunday, April 24, at 2:14 p.m.

23 Q. Do you see under where it says "Hello Josh Schulte"?

24 A. Yes.

25 Q. What's the product that was shipped?

K2D3SCH3

Berger - Direct

1 A. The Inatek USB 3.0 SATA.

2 Q. All right. What does it say under "arriving"?

3 A. It say it's arriving Sunday, April 24.

4 Q. Of what year?

5 A. 2016.

6 Q. Let's take a look at the next slide, please. What are we
7 looking at here?

8 A. So this is a file information for a particular file that
9 was found on the defendant's computer.

10 Q. What's the file that was found?

11 A. The file itself is Tails-I386-2.2.1.torrent.

12 Q. We talked a little bit about Tails before. What is that?

13 A. So Tails is an operating system that allows you to connect
14 directly to the Tor network. It's unique in that it -- one of
15 its capabilities is it forces all of your traffic to go
16 directly through the Tor network.

17 Q. How does it work?

18 A. So you would download the Tails file. You would then copy
19 the data on to some kind of removable media, so maybe a DVD or
20 a USB drive. You would then power off your computer and turn
21 it back on, and you would indicate for your computer to boot
22 from that device. Instead of loading the operating system like
23 Windows that you would normally boot into, you would boot into
24 an operating system running from this device.

25 Q. What's the impact of booting from the device rather than

K2D3SCH3

Berger - Direct

1 from your regular operating system?

2 A. So by booting from this device, the entire operating system
3 is loaded into memory. And everything about Tails is designed
4 to operate inside of memory and not touch the hard drive.

5 Q. So, if you were using Tails, would there be signs on your
6 hard drive of the activity you were doing?

7 A. No, there would not.

8 Q. Can you use Tails with a virtual machine?

9 A. You can create a virtual machine of Tails, yes.

10 Q. Are you, when you are in a virtual machine, are you able to
11 bring data in from your regular computer?

12 A. Yes, you can.

13 Q. Are you familiar with the concept mounting?

14 A. Yes.

15 Q. What's mounting?

16 A. So mounting is in the Linux operating system, if you want
17 to connect to data on another computer or a server you have to
18 mount the data. So you connect to that particular share of
19 data, and you assign the mount point on your system. It would
20 just be an empty folder. Once you mount it, if you go into
21 that folder, you would be looking at the data on the other
22 system or the server.

23 Q. Can you tell when the Tails file was downloaded?

24 A. Yes.

25 Q. When is that?

K2D3SCH3

Berger - Direct

1 A. April 24, 2016, at 5:02 p.m. local time.

2 Q. How do you know that's the date?

3 A. You can see here on the last written entry.

4 Q. Do you also see an entry for file created?

5 A. Yes, I do.

6 Q. What's listed there?

7 A. May 10, 2016 at 9:06 p.m.

8 Q. Is there a reason why the file created date is listed as
9 May 10 versus April 24?

10 A. Yes.

11 Q. What's that?

12 A. This is generally what happens when you download a file,
13 and you move the file from one piece of media to another piece
14 of media. The way file systems metadata works, the last
15 written or last modified date is generally preserved when you
16 copy files from one system to another. However, the other
17 attributes are generally recreated.

18 So if you have this file on a thumb drive, and you
19 copy it over to the computer, the file on the computer would
20 have a creation and a last accessed of the most recent time.
21 However, the last modified or last written date would be
22 preserved in that transfer.

23 Q. Did you see any evidence that the defendant had engaged in
24 that kind of copying activity on his home network?

25 A. Yes.

K2D3SCH3

Berger - Direct

1 Q. Could you explain, please.

2 A. So, the computer we looked at, particularly the C drive,
3 had activity on it where there were files shown to have been
4 last modified at a point prior in time to when there was
5 indication that the drive was reformatted.

6 Q. Let's take a look, you have it in front of you at
7 Government Exhibit 1603, a thumb drive recovered from the
8 defendant's apartment.

9 A. Yes.

10 Q. You can take it out of the bag. You ever seen Government
11 Exhibit 1603 before?

12 A. Yes.

13 Q. How do you recognize it?

14 A. I have my initials on the evidence item.

15 Q. Have you reviewed a forensic image of that thumb drive?

16 A. Yes, I have.

17 Q. Were there any programs on there?

18 A. Yes, there were.

19 Q. Which programs?

20 A. The program Eraser Portable.

21 Q. What's Eraser Portable?

22 A. So Eraser is a program that's designed to securely delete
23 files. Eraser Portable is a slightly modified version of the
24 program that allows it to run off of a piece of removable media
25 without being installed on the computer.

K2D3SCH3

Berger - Direct

1 Q. When you say "securely erase," what are you referring to?

2 A. So, the way a file is normally deleted would not be
3 considered secure. The way files are stored on your system,
4 you can think about it as a table of contents that points to
5 where files are. Generally when you delete a file, the file is
6 marked in the table of contents as being deleted. So the
7 operating system no longer would show you that file, but the
8 data for the file is still there and is able to be recovered
9 with forensic software.

10 Securely deleting a file would go to the location on
11 the hard drive where the content of that file is stored, and
12 overwrite that data.

13 Q. Take a look at the next slide, please. What are we looking
14 at here?

15 A. So this a screenshot from a forensic program showing the
16 basic folder structure and some files from that thumb drive.

17 Q. Can you explain the folder structure.

18 A. So at the top here, we have this Eraser Portable directory.
19 Within the Eraser Portable directory, there is an app
20 directory, a data directory, and an other. Within the data
21 directory there is a settings directory, that stores
22 information about the program, certain configuration options,
23 things related to its activity. Within the Eraser directory
24 under the app directory, which is here, that's where the actual
25 program itself resides.

K2D3SCH3

Berger - Direct

1 Q. Do you see a file called schedlog.txt?

2 A. Yes, I do.

3 Q. What's that file?

4 A. So that is a log file that records, among other things,
5 when Eraser Portable starts and stops.

6 Q. Did you look at the schedlog file?

7 A. Yes, I did.

8 Q. Let's go to the next slide, please. What's this?

9 A. This is the content of the schedlog file.

10 Q. Does it show that the Eraser Portable program was opened on
11 the thumb drive in 2016?

12 A. Yes, it does.

13 Q. When was it first opened?

14 A. It was first opened on April 23, 2016, at 6:12 p.m.

15 Q. Was the program ever closed?

16 A. Yes, it was.

17 Q. When was it closed?

18 A. April 28, 2016, at 8:36 p.m.

19 Q. So, during that five-day period, was the Eraser Portable
20 program running?

21 A. Yes.

22 Q. Have you looked at the program's activity during that
23 period?

24 A. Yes.

25 Q. Can we look at the next slide, please. What are we looking

K2D3SCH3

Berger - Direct

1 at here?

2 A. This is a screenshot from a forensic program showing the
3 app directory. You can see here that there is a series of
4 files, some of which are overwritten or partially overwritten,
5 and their corresponding file date -- the date and time of those
6 files.

7 Q. Which ones are the overwritten files?

8 A. So you can see here, the -- let me circle it. You see that
9 little icon there. It's got a -- little hard to see here. A
10 little red in the bottom-right hand of that icon. That
11 indicates that it's deleted or overwritten.

12 Q. So, you see that entrance for default.ers?

13 A. Yes.

14 Q. What's that kind of file?

15 A. So the default.ers file is a file that's used with Eraser
16 Portable. It keeps track of entries in the queue or jobs for
17 Eraser to conduct.

18 Q. So as part of your analysis, did you examine the default
19 file?

20 A. Yes, I did.

21 Q. Were there any particular properties of the file that you
22 focused on?

23 A. Yes.

24 Q. What were those?

25 A. The size of the file.

K2D3SCH3

Berger - Direct

1 Q. Why did you focus on size of the file?

2 A. So the file, the default.ers file, the file size is
3 directly proportional to the entries that are entered into the
4 Eraser program.

5 Q. To be clear, is there a relationship between the size of
6 the file and the underlying file that the program is trying to
7 delete?

8 A. Yes. So the files that you would add into Eraser, the
9 files you were trying to delete, those pads to those files are
10 stored in this file. So as you would put more files in, or
11 have files that have longer pads, the default.ers file would
12 grow.

13 (Continued on next page)

14

15

16

17

18

19

20

21

22

23

24

25

K2dWsch4

Berger - Direct

1 BY MR. KAMARAJU:

2 Q. And for purposes of the size of the default file, does it
3 matter how big the actual file that you're trying to delete is?

4 A. No.

5 MR. KAMARAJU: Let's take a look at the next slide,
6 please.

7 Q. What are we looking at here?

8 A. So, these are two different entries that were on the drive,
9 listed under default.ers. They each have different files that
10 were listed in that queue.

11 Q. Could you identify the files that were listed in the queue
12 in the top selection?

13 A. So, on the top, we -- there is a -- there are two folders,
14 Brutal Kangaroo and ArrayList. On the bottom, there are five
15 files. They're data6.bkp, data5.bkp, data4.bkp, data3.bkp, and
16 data2.bkp.

17 Q. From the file pack, can you tell what drive these documents
18 are -- sorry, these files were on?

19 A. Yes. They were on the D drive.

20 Q. Now, you testified about the size of the default.ers file.
21 Is there a relationship there between the file path size and
22 the size of the file?

23 A. Yes.

24 Q. So when you type in, for example, Brutal Kangaroo versus
25 ArrayList, will the file size be different?

K2dWsch4

Berger - Direct

1 A. Yes, it would.

2 Q. And have you heard testimony about Brutal Kangaroo before?

3 A. Yes.

4 Q. What's your understanding of what Brutal Kangaroo is?

5 A. My understanding is it is a project that was worked on at
6 the CIA.

7 Q. And who worked on it at the CIA?

8 A. Josh Schulte.

9 Q. And the naming convention, data.bkp -- data 1, data 2, data
10 3, data 4 -- did you see that naming convention used anywhere
11 else on the defendant's computer?

12 A. Yes.

13 Q. Where was that?

14 A. That would be in the container that he used for encrypted
15 data within the search engine.

16 MR. KAMARAJU: Let's take a look at the next document.

17 Q. Can you tell us what we're looking at here?

18 A. This is a demonstration of how Eraser Portable looks. You
19 can see when the program is open there is an area where you
20 would add files. On this particular screenshot, the folder
21 ArrayList is in that list.

22 MR. KAMARAJU: Let's look at the next one.

23 Q. What's reflected here?

24 A. So, this reflects both the ArrayList folder and the Brutal
25 Kangaroo folder added.

K2dWsch4

Berger - Direct

1 Q. And on the left side of those file paths, where it says D
2 colon --

3 A. Yes.

4 Q. -- what does that reflect?

5 A. That represents the -- the D represents the drive those
6 files reside on, and then everything else is the folders and
7 subfolders that they belong to.

8 MR. KAMARAJU: OK. Let's look at the next slide.

9 Q. What are we looking at here?

10 A. So, this represents those five BKP files being added into
11 the Eraser program.

12 Q. Now, did you examine that the way the default ERS reacted
13 when you were entering these steps?

14 A. Yes.

15 Q. Did that match the forensic evidence you saw in the Eraser
16 Portable thumb drive?

17 A. Yes.

18 Q. Did you arrive at any conclusions about how the defendant
19 used Eraser Portable between April 23 and April 28, 2016?

20 A. Yes.

21 MR. KAMARAJU: Let's take a look at those. Can we go
22 to the next slide, please.

23 Q. Let's just start with April 23. What happened then?

24 A. On April 23, at 6:12 p.m., the defendant opens Eraser
25 Portable.

K2dWsch4

Berger - Direct

1 Q. What happens next?

2 A. By 6:14, so two minutes later, the ArrayList item had been
3 added to the queue for removal.

4 Q. And generally speaking, how did you arrive at that
5 conclusion?

6 A. So, we looked at the activity in the over, partially
7 overwritten and deleted files and their file sizes.

8 Q. What's the next thing that happened?

9 A. So, at April 23, by 6:20 p.m., both Brutal Kangaroo and
10 ArrayList had been added to that queue.

11 Q. Now, do you see there's an entry, or there's a line there
12 that's marked off in blue?

13 A. Yes.

14 Q. Now, the events that are marked off in blue, were you able
15 to tell the order in which those events occurred?

16 A. No.

17 Q. Why is that?

18 A. It's just the nature of how the program works.

19 Q. So without referencing the order, what were the events that
20 occurred during that time?

21 A. So, the two things that happened were the Eraser program
22 was run on the Brutal Kangaroo and ArrayList folders; that
23 means they were deleted. And the five BKP files were added to
24 the queue.

25 Q. And were those files that were deleted using Eraser

K2dWsch4

Berger - Direct

1 Portable, the dot-BKP files?

2 A. No.

3 Q. How do you know that?

4 A. Because, again, the way the file operates and they were
5 still in that ERS file when the program was closed out.

6 Q. And when was the program closed out?

7 A. On April 28, 2016, at 8:36 p.m.

8 Q. Does Eraser Portable securely delete all the files on a
9 hard drive or just specific files?

10 A. Just the specific files you tell it to.

11 Q. Are there programs that securely wipe the entire hard
12 drive?

13 A. Yes, there are.

14 Q. Did you find any forensic evidence of any of those types of
15 programs on the defendant's home network?

16 A. Yes.

17 Q. What programs did you find?

18 A. The program is named Darik's Boot and Nuke, also referred
19 to as DBAN.

20 MR. KAMARAJU: Can we go to the next slide.

21 Q. What are we looking at here?

22 A. So, this is from a forensic program looking at the file
23 information before the file containing DBAN.

24 Q. When was DBAN downloaded?

25 A. DBAN was downloaded on April 30, 2016, at 11:28 a.m.

K2dWsch4

Berger - Direct

1 Q. Do you see the file-created date?

2 A. Yes.

3 Q. What's listed there?

4 A. May 5, 2016, at 9:59 p.m.

5 Q. Why is that date, May 5, if DBAN was downloaded on April
6 30?

7 A. Same as what we've, what I talked about earlier. If you
8 move files from one drive to another, specifically one that
9 maybe was reformatted, generally the last modified or
10 last-written time is preserved across that transfer.

11 Q. Do you see the row there at the top that says file EXT and
12 then it says ISO?

13 A. Yes.

14 Q. What's an ISO file?

15 A. So, ISO file is a type of file. It's generally used for
16 the contents of disk images, such as DVDs, CDs or image for a
17 USB thumb drive.

18 Q. What happens if you click on the ISO file?

19 A. Depends what software is installed on your computer. If
20 you don't have the appropriate software, then you're not going
21 to be able to view it on this.

22 Q. If you are successfully able to open an ISO file, what
23 happens next?

24 A. You could view the contents that are contained within the
25 file, or you could also view it in a program that would allow

K2dWsch4

Berger - Direct

1 you to write it to some kind of removal media, so a DVD or a
2 thumb drive.

3 Q. Did you access this ISO file?

4 A. Yes, I did.

5 MR. KAMARAJU: Let's take a look at the next slide.

6 Q. What are we looking at here?

7 A. So, I took the ISO and booted it up in a virtual machine,
8 and this is the screen that shows up when you power it up.

9 Q. Do you see the red "warning" label under Darik's Boot and
10 Nuke?

11 A. Yes.

12 Q. Could you read that, please?

13 A. Sure. It says: "Warning. This software irrevocably
14 destroys data."

15 Q. What's that mean?

16 A. That means that it would securely erase data where, in a
17 way that you cannot recover the data.

18 Q. And do you see down below where it says, "Press the F2 key
19 to learn about DBAN"?

20 A. Yes.

21 Q. Did you press the F2 key?

22 A. I did.

23 MR. KAMARAJU: Let's take a look.

24 Q. What's this?

25 A. So, this is a screen that displays more information about

K2dWsch4

Berger - Direct

1 the program.

2 Q. Could you read the first paragraph, please?

3 A. "Darik's Boot and Nuke (DBAN) is a self-contained boot
4 floppy that securely wipes the hard disks of most computers.
5 DBAN will automatically and completely delete the contents of
6 any hard disk that it can detect, which makes it an appropriate
7 utility for bulk or emergency data destruction."

8 Q. Let's start at the top. What's a self-contained boot
9 floppy?

10 A. Similar to how we described Tails earlier, you would take
11 the contents, put it on some kind of removable media and you
12 can boot off of it. It's a self-contained operating system.
13 It does not require an operating system to have been present on
14 the computer in order to utilize this.

15 Q. What does it mean to securely wipe a hard disk?

16 A. So, as I talked about earlier, wiping a hard disk securely
17 is the same as wiping a file securely. It's the difference
18 between deleting it and just marking it as deleted or going
19 over every single possible space on the hard drive and
20 overwriting it.

21 Usually when you securely wipe a hard drive, you overwrite
22 it with either all zeros or all random data.

23 Q. On Government Exhibits 1609 and 1610, the hard drives we
24 looked at before, did you see any data on those?

25 A. No, I did not.

K2dWsch4

Berger - Direct

1 Q. Could you read the next line?

2 A. "This program clears directly attached IDE, PATA, SATA,
3 SCSI and SAS disks. Some USB and IEEE 1394 (Firewire) devices
4 may be recognized. DBAN requires a computer with a PCI bus and
5 32 megabytes of memory."

6 Q. So the acronyms in the first sentence, the ones starting
7 with IDE and going forward, what do those represent?

8 A. Those just refer to different types of hard drive
9 interfaces.

10 Q. Do you see the one called SATA?

11 A. Yes.

12 Q. Have we heard that term before?

13 A. Yes, we have.

14 Q. OK. When?

15 A. When we were talking about the hard drives that are in
16 front of me here.

17 MR. KAMARAJU: Let's take a look at the next slide.

18 Q. What's this?

19 A. So, this is another information screen that's present from
20 the DBAN menu.

21 Q. And what information is it presenting?

22 A. It shows different options you can use to wipe hard drives.

23 Q. Now, were you able to also examine any of the log-in
24 activity on the defendant's home network?

25 A. Yes.

K2dWsch4

Berger - Direct

1 MR. KAMARAJU: Let's go to the next slide, please.

2 Q. I'd like to focus on April 30 to May 1, 2016. OK?

3 A. OK.

4 Q. Were you able to look at data from those dates?

5 A. Yes.

6 Q. Now, is this the auth.log file again?

7 A. This is the auth.log file. I believe we were looking at
8 the auth.log 1 file, which is just a rollover of the auth.log
9 file when it gets to a certain size.

10 Q. Remind us what the auth.log file is.

11 A. The auth.log just stores authenticated events.

12 Q. Looking at this file, are you able to tell whether the
13 defendant logged in to his virtual machine on April 30, 2016?

14 A. Yes.

15 Q. How do you know?

16 A. Just going to circle a line right here.

17 So, those lines that indicate cinnamon-screensaver-dialog
18 gkr-pam unlocked login keyring, that's an indication that the
19 screen saver for the virtual machine was unlocked with a
20 password.

21 Q. Let's just walk through that. What is a
22 cinnamon-screensaver?

23 A. Cinnamon refers to the graphical user interface that was
24 present on the virtual machine.

25 Screen saver is -- was very common in older computers where

K2dWsch4

Berger - Direct

1 you had to worry about screen burn-in if you left your computer
2 on the same data for a long period of time. So after a few
3 minutes, the screen saver would kick in and just animate
4 something to prevent screen burn-in. Now they're more common
5 to prevent unauthorized access to a computer, so when you're
6 away from your computer for a few minutes, it might lock and
7 then require you to unlock it when you return to your computer.

8 MR. KAMARAJU: Let's turn to the next slide.

9 Q. What's this?

10 A. This is just more activity also contained in the auth.log.

11 Q. Specifically, were you able to tell if the defendant logged
12 in to his VM on May 1, 2016?

13 A. Yes.

14 Q. And how do we know that?

15 A. Again, I'll circle it here.

16 There is additional entries displaying how the screen saver
17 was unlocked during this time.

18 Q. So what times did the defendant log in to his virtual
19 machine?

20 A. There's an entry on May 1 at 1:57 a.m. There's another
21 entry later that morning, at 2:34 a.m. There's one at 2:56
22 a.m. and again at 3:18 a.m.

23 Q. Remember we talked a little about mounting data into your
24 VM?

25 A. Yes.

K2dWsch4

Berger - Direct

1 Q. Between April 30 and May 1 of 2016, did the defendant mount
2 any data into his VM?

3 A. Yes.

4 Q. What did he mount?

5 A. On May 1, he mounted a folder on his computer.
6 Specifically, the D drive on his computer was connected into
7 the virtual machine.

8 Q. And the data.bkp files we looked at before, were those
9 saved in his D drive?

10 A. Yes.

11 MR. KAMARAJU: Let's take a look at the next slide.

12 Q. Did you look at any additional Google searches that the
13 defendant did?

14 A. Yes.

15 Q. Did you look at searches that he did between the evening of
16 April 30, 2016, and May 1, 2016?

17 A. Yes.

18 MR. KAMARAJU: Let's go to the next slide.

19 Q. What are these?

20 A. So, these are those additional Google searches, starting on
21 May 1, 2016, at 2:51 a.m. UTC time.

22 Q. Let's start at the one all the way at the bottom. What's
23 the date and time of that search?

24 A. The date and time is May 1, 2016, 2:51 a.m. UTC. So if we
25 go back four hours, that's going to be on the evening of April

K2dWsch4

Berger - Direct

1 30, 2016, at 10:51 p.m.

2 Q. And what did the defendant search for?

3 A. He searched for Western Digital disk wipe utility.

4 Q. What's Western Digital?

5 A. It's a hard drive manufacturer.

6 Q. Government Exhibits 1609 and 1610, what's the manufacturer
7 of those hard drives?

8 A. For 1610, it's a Western Digital drive. And for 1609, it's
9 also a Western Digital drive.

10 Q. Now, what's a disk-wipe utility?

11 A. It's a utility similar to what we talked about with DBAN.
12 It's a utility that allows you to wipe a drive.

13 Q. Let's move up a little bit. Do you see how that same
14 search the search for Western Digital disk wipe utility, is
15 repeated a few times?

16 A. Yes.

17 Q. Do you have an understanding as to why that is?

18 A. One possibility would have been if you searched for
19 something in Google and you see the results, you visit those
20 pages and then you go back to your search results. Sometimes
21 when you go back, the looking at your results might trigger
22 Google to record it as another search.

23 Q. Let's take a look at one of the different ones. Do you see
24 an entry for May 1, 2016, at 02:55:27 UTC?

25 A. Yes.

K2dWsch4

Berger - Direct

1 Q. And remind us. What's that in local time?

2 A. That would on the evening of April 30, 2016, at 10:55 p.m.
3 local time.

4 Q. What did the defendant search for there?

5 A. He searched for a Samsung SSD wipe utility.

6 Q. What's a Samsung SSD?

7 A. So, Samsung is another hard drive manufacturer. The SSD
8 refers to a type of hard drive. Conventional hard drives, such
9 as the two up here, have what's called platters in them. They
10 are disks that spin at a high rate of speed, and there's an arm
11 that goes across those drives and magnetically reads and writes
12 data to them.

13 SSD is a solid state drive. There are no moving parts.
14 Everything is stored on internal circuitry.

15 Q. What's a Samsung SSD?

16 A. That would be a utility to wipe a Samsung SSD drive.

17 Q. Did the defendant's home network include any Samsung SSDs?

18 A. Yes, it did.

19 Q. Where?

20 A. The C drive, or the primary drive of the workstation, was a
21 Samsung SSD drive.

22 MR. KAMARAJU: Let's take a look at the next slide.

23 Q. What are we looking at here?

24 A. These are more Google searches.

25 Q. Let's start at the bottom. What's the date and time of the

K2dWsch4

Berger - Direct

1 bottom search?

2 A. 2016, May 1, 7:18 UTC, so that would be 3:18 a.m.

3 Q. And what's the search?

4 A. The search was "how long does it take to calculate MD5."

5 Q. What's MD5?

6 A. So, MD5 is a type of hash algorithm.

7 Q. Remind us. What is a hash algorithm?

8 A. It's used to generate a unique fingerprint of a file.

9 Q. What does it mean to calculate MD5?

10 A. So, in order to generate that MD5, there is a mathematical
11 computation that has to take place. We talked about the MD5
12 algorithm. You feed data into it and the output is that value.
13 Inside that algorithm, there is a lot of mathematical
14 computation that's going on.

15 Q. And what gets spit out at the end of that?

16 A. A value that looks like a bunch of letters and numbers.

17 Q. How do you typically use that hash value?

18 A. So, you can use it in a couple different ways. In -- one
19 way would be to look at two files that look very similar to
20 each other, you want to know if they're identical.

21 Another way is if you're transferring data. If you're
22 sending data from one person to another, you might hash the
23 file before you send it, generate that fingerprint. You then
24 send the file to another person. Once they've received the
25 file, you could ask them to calculate the MD5, and then you can

K2dWsch4

Berger - Direct

1 see if they match. If they match, then you know the file was
2 transferred successfully.

3 Q. Let's go two entries up. Do you the line that says
4 07:18:45 UTC?

5 A. Yes.

6 Q. And what's that in local time?

7 A. That's going to be 3:18 a.m.

8 Q. And what website was visited there?

9 A. He visited a site researchgate.net, and it was a post
10 entitled "What Is the Fastest Way to Hash MD5 Large Files?"

11 Q. Is there any correlation between the calculation of an MD5
12 file and the size of the files you're trying to hash?

13 A. Yes.

14 Q. What is it?

15 A. So, because a hashing has to take into account the entirety
16 of the file, as the file gets bigger, there's more computation
17 that has to take place.

18 Q. Let's take a look at the next one up. What's the date and
19 time there?

20 A. So, that's May 1, 2016, 7:21 UTC, so that's going to be
21 3:21 a.m.

22 Q. What website was visited there?

23 A. That website was superuser.com, and it looks like an
24 article entitled "How Can I Verify That a 1TB File Transferred
25 Correctly?"

K2dWsch4

Berger - Direct

1 Q. Do you understand what the reference to TB is?

2 A. Yeah, I understand that to refer to a terabyte.

3 Q. What's a terabyte?

4 A. It's a measure of data size.

5 Q. And how big is it?

6 A. It's fairly large.

7 Q. Is it -- could you compare it to megabytes, for example?

8 A. Sure. So, if you have -- I'm sorry.

9 If you have a megabyte of data, if you have a thousand
10 megabytes, you would have what is known as a gigabyte. If you
11 have a thousand gigabytes, you would have a terabyte.

12 Q. Now, during the time of -- withdrawn.

13 Did you hear Mr. Leedom testify about the size of the
14 Confluence and Stash backups?

15 A. Yes.

16 Q. Do you recall roughly how large he testified those would be
17 when unzipped?

18 A. I believe they -- he referred to them as being several
19 hundred gigabytes in size.

20 Q. Are those large files, generally speaking?

21 A. Those are pretty large.

22 MR. KAMARAJU: Let's take a look at the next --

23 Q. Before we go there, was the defendant logged in to his VM
24 at the time of these searches?

25 A. Yes.

K2dWsch4

Berger - Direct

1 MR. KAMARAJU: Let's take a look at the next slide.

2 Q. Are you familiar with a concept known as reformatting a
3 computer?

4 A. Yes.

5 Q. What is that, generally?

6 A. So, on each hard drive, there's a concept of a file system.
7 This is what I referred to earlier, where you have the table of
8 contents and refers to all the files on the hard drive. When
9 you reformat a hard drive, you're essentially creating an
10 entirely new file system, so that table of contents gets
11 completely reinitialized; it doesn't know about any of the
12 previous data that's on the drive.

13 MR. KAMARAJU: Let's take a look at the next slide.

14 Q. What's this?

15 A. So, this is a view of the, what's known as the MFT file on
16 the defendant's C drive in the forensic program.

17 Q. All right. So let's walk through it. See the name at the
18 top, dollar sign MFT?

19 A. Yes.

20 Q. What is that?

21 A. So, the MFT file is known as the master file table. The
22 type of file system refers to an NCFS use of this. This is
23 what keeps track of all the files on the file system.

24 Q. Do you see how all the last accessed, the file created and
25 last-written dates are all May 5, 2016, at 11:15:57 p.m.?

K2dWsch4

Berger - Direct

1 A. Yes.

2 Q. What conclusions do you draw from that?

3 A. That the MFT file was created at that time due to the drive
4 being reformatted.

5 Q. And which drive is this?

6 A. This is the C drive.

7 Q. Was that the Samsung SSD that you referred to before?

8 A. Yes.

9 MR. KAMARAJU: Let's take a look at the next slide.

10 Q. What do we see here?

11 A. So, this is similar. We're looking at the information for
12 the MFT file on the D drive.

13 Q. And what happened to that file on May 5, 2016?

14 A. It was also shows -- it shows that it was created at 8:01
15 p.m. on May 5.

16 Q. What does that mean?

17 A. Again, with the MFT file being newly created, that would
18 indicate that that volume was reformatted.

19 Q. See where it says RAID 5?

20 A. Yes.

21 Q. What is that in reference to?

22 A. That's in reference to what I talked about earlier. The
23 other three drives in the computer were connected in what's
24 known as a RAID volume or RAID 5 volume. They're hooked in a
25 way that they're presented to the operating system as a single

K2dWsch4

Berger - Direct

1 drive. In this case they present as a single D drive.

2 Q. What was the impact of the defendant reformatting his
3 computer on May 5, 2016?

4 A. You would not be able to easily access any data that was on
5 the drive previously.

6 MR. KAMARAJU: Let's go to the next slide.

7 Q. Just to recap, let's walk through. What happened on April
8 23, 2016?

9 A. The defendant opened Eraser Portable for the first time.

10 Q. What happened next?

11 A. On April 24, the defendant ordered a SATA adapter and
12 downloaded Tails onto his computer.

13 Q. Just remind us again what Tails is.

14 A. Tails is an operating system that directly connects you
15 into the TOR network.

16 Q. What happened next?

17 A. So, on April 28, 2016, by this time, the defendant had used
18 Eraser Portable to securely delete two folders on the
19 computer -- Brutal Kangaroo and ArrayList -- and had started
20 the process of deleting five BKP files but did not complete it.

21 Q. What's the next thing that happened?

22 A. So, on April 30, the defendant downloaded the Darik's Boot
23 and Nuke program, which is used to securely delete hard drives.
24 Between 10:51 and 10:55 on April 30, there were searches
25 performed, including "how to kill your data dead with these

K2dWsch4

Berger - Direct

1 tips and tools" and "wipe" utilities for Samsung and Western
2 Digital hard drives.

3 Q. What happened next?

4 A. From April 30 into May 1, so late on the 30th, the
5 defendant periodically would unlock the screen saver to his
6 virtual machine, indicating he was logged on. Around 3 a.m. on
7 May 1, the defendant performed a search for "how I can verify
8 that a one terabyte file transferred correctly." In addition,
9 he also searched for ways to hash data.

10 Q. What's the next thing that happened?

11 A. On May 5, 2016, both drives, the C and the D drive, were
12 reformatted.

13 Q. What's the impact of that?

14 A. That would make it difficult to recover data that would
15 have been on those drives previously.

16 MR. KAMARAJU: Your Honor, no further questions at
17 this time.

18 THE COURT: All right. Ms. Shroff.

19 MR. BRANDEN: Judge, I'll be doing the cross.

20 THE COURT: Mr. Branden.

21 MR. BRANDEN: Is now a good time for lunch?

22 THE COURT: No.

23 MR. BRANDEN: I'd like to integrate some comments that
24 I heard from the direct testimony.

25 THE COURT: OK. Why don't you start. We'll break at

K2dWsch4

Berger - Cross

1 1:00.

2 CROSS-EXAMINATION

3 BY MR. BRANDEN:

4 Q. Good afternoon, Mr. Berger. I'm Jim Branden. How are you?

5 A. I'm all right.

6 Q. Good.

7 For the most part, I'm just going to make a review of your
8 demonstrative and go over some of those slides, hopefully in
9 order, so we stay in the same rhythm that the government
10 started us off on.

11 MR. BRANDEN: First of all, can we see slide No. 6,
12 please.

13 Q. You testified about this slide. This appears to be from
14 Anthony Leonis, correct?

15 A. Yes.

16 Q. To Joshua Schulte, correct?

17 A. Yes.

18 MR. BRANDEN: And others are cc'd.

19 And may I see slide 5 as well.

20 Q. OK. This slide, if I'm correct, preceded the one we just
21 looked at from Anthony Leonis, correct?

22 A. Yes.

23 Q. And in this slide, Mr. Schulte is explaining why he
24 believes that he should still be an admin on OSB libraries,
25 correct?

K2dWsch4

Berger - Cross

1 A. Yes.

2 Q. He's making a case for himself there, correct?

3 A. It appears that way, yes.

4 MR. BRANDEN: OK. And then if we go again to No. 6,
5 and the body of that is in 7, I believe.

6 Q. And here is Mr. Leonis's response, correct?

7 A. Yes.

8 Q. Does Mr. Leonis directly say that Mr. Schulte cannot be an
9 admin systems administrator at OSB?

10 A. On this slide?

11 Q. Uh-huh.

12 A. No.

13 Q. No. All he says, correct me if I'm wrong, is that Jojo has
14 been brought on to manage it, correct?

15 A. Correct.

16 Q. But he doesn't say directly that Mr. Schulte cannot be the
17 systems administrator?

18 A. Correct.

19 Q. OK. So that would appear to be still an open question,
20 correct?

21 A. Based on only this slide?

22 Q. Uh-huh.

23 A. Yes.

24 Q. OK. Now, moving on further to the date line that you
25 established with regard to the Vault 7 and Vault 8 release on

K2dWsch4

Berger - Cross

1 WikiLeaks, there are some certain limitations to the value in
2 your report with regard to that, and I'll click them off. I
3 believe that you would agree that the report did not purport to
4 identify the date the data was exfiltrated from the CIA, is
5 that correct?

6 A. At the time the report was written, yes, that's correct.

7 Q. OK. And secondly, other than the analysis of the four data
8 points that you talked about on direct -- two of which were in
9 Confluence, two of which were in Stash -- the report did not
10 analyze the contents of the data on WikiLeaks to confirm with
11 100 percent certainty on a match to the data within the CIA
12 DevLAN database, is that correct?

13 A. That's correct.

14 Q. And third, it was unclear, for purposes of the report,
15 whether the times listed therein were Eastern Standard Times or
16 not, correct?

17 A. At the time of the report, yes.

18 Q. Uh-huh. OK. So that interested me. I'm not sure that it
19 is a pivotal point, but the window that you ultimately
20 determined in Confluence that you found was the operable
21 window, that the materials were taken from that 3/2, 3/3 date
22 was from March 2, 2016 at 3:58 p.m. to March 3, 2016, at 6:47
23 a.m., correct?

24 A. Correct.

25 Q. And the backup was at 6:29 Eastern Standard Time, right?

K2dWsch4

Berger - Cross

1 A. Correct.

2 Q. So would the fact that you don't know whether those other
3 times, meaning the window times, were Eastern Standard Time
4 affect the analysis?

5 A. If you're asking me at the time of the report what I knew?

6 Q. Uh-huh.

7 A. At the time of the report, we didn't know what time zone
8 the times in the database were using, correct.

9 Q. So what I'm saying is if there's a four-hour switch, right,
10 from whatever Zulu time is versus Eastern Standard Time, it may
11 be that the backup from 6:29 on March 3 does not actually fit
12 within your window? Correct?

13 A. Incorrect.

14 Q. And why is that?

15 A. It has to do with how the backup files were named.

16 Q. I guess I'll have to take your word. I don't really know
17 what that means. Can you just elaborate a little bit?

18 A. I can elaborate.

19 Q. Sure. Please.

20 A. So, Mr. Leedom testified yet about how the backups were
21 generated on the Atlassian products. Specifically, he showed
22 the screenshot of what was referred to as a backup script.
23 This was a program that ran each day at a specific time to
24 generate the backups on each system.

25 Part of that script was to generate the file name for the

K2dWsch4

Berger - Cross

1 backups. So as we've seen the screenshot several times, both
2 the SQL and TGZ files, they had the Confluence and they had a
3 time stamp in the file name. That was generated in the script.
4 The way the script did that is it made a call to the system to
5 get the current system time. It then took that time and
6 embedded it inside the name of the file. I believe the
7 Confluence times had that time of 0625, which I testified that
8 indicated the beginning of the backup script, and I believe it
9 took about three or four minutes to run. And that's why the
10 last modified time was 6:29 a.m. Because that time is
11 indicated in the file name and that matches the times of the
12 files we're looking at when we're looking at them in a computer
13 on Eastern Standard Time, we can conclude that that computer
14 was, in fact, set to eastern time.

15 Q. OK. Thank you for that.

16 A. You're welcome.

17 MR. BRANDEN: Now I'd like to look briefly at slide
18 23, if I may.

19 Q. You testified at some length about this slide, and in
20 particular, you commented on the PrevVer number, correct?

21 A. Correct.

22 Q. And that number ends in 129, correct?

23 A. Correct.

24 Q. And there were 17 versions of Michael R.'s home, and I
25 think it's your testimony that the 17th version is the one that

K2dWsch4

Berger - Cross

1 appears on WikiLeaks, correct?

2 A. Correct.

3 MR. BRANDEN: And now the next page, please, 24.

4 Q. And here we have, I guess this is a screenshot; is that
5 what you would call this?

6 A. Yes.

7 Q. From the WikiLeaks release?

8 A. Yes.

9 Q. OK. And it shows that this is the 17th version of Michael
10 R.'s home and that there were 16 previous versions, correct?

11 A. Correct.

12 Q. And the PrevVer number is on this page on the line that
13 begins with "local host," correct --

14 A. Correct.

15 Q. -- at the top?

16 But above that there's a separate number, which is just one
17 number higher than the 129?

18 A. Yes.

19 Q. It's 3375130. Can you tell me why that number's there?

20 A. So, being as how the page was entitled "Michael R.'s Home,"
21 and it shows that on WikiLeaks's site, it seems that WikiLeaks
22 changed it. They appear to have done that to redact the name
23 Michael R. In doing so, they replaced it with that number that
24 ends in 130.

25 Q. Now, at the time that you prepared your initial report from

K2dWsch4

Berger - Cross

1 which your demonstrative is drawn, you were already informed,
2 were you not, that people at the CIA or people at the FBI
3 believed that the leak occurred -- the leaked materials were
4 from around March 2 or March 3? Is that correct?

5 A. Yeah. I was given an idea of when they thought the data
6 was from, yes.

7 Q. So in a sense, your report was really just a confirmatory
8 report?

9 A. It was a report to go investigate what happened and confirm
10 it, but it wasn't that I took what they said and just put it on
11 paper. I went and did my own investigation.

12 Q. And during your investigation in the matter, did you come
13 to learn that at some point there had been a different date
14 that was suggested for the date of the materials, the Vault 7,
15 Vault 8 materials?

16 A. I had heard early on in the investigation of different
17 dates, yes.

18 Q. And do you remember what that date was?

19 A. I think it was around March 7th or 8th, I believe.

20 Q. OK. So the initial date that was suggested as a possible
21 date to WikiLeaks was March 8, but it was modified by you and
22 others back to the 2nd or 3rd, is that correct?

23 A. I didn't modify anything. I didn't make that determination
24 of March 7th or 8th.

25 Q. And no one has read through what's on WikiLeaks and

K2dWsch4

1 compared it to the materials in Confluence and Stash; it's just
2 that you've used these data points to determine the window?

3 A. You mean no one's read through the data in its entirety?

4 Q. Yes.

5 A. I don't know. I have not read all 10,000 pages, no.

6 Q. And further, there's nothing in the report that would tie
7 it to a particular user of Confluence or Stash, correct?

8 A. I don't believe so, no.

9 Q. Would you agree that one of the purposes of Stash is to
10 store old versions of files?

11 A. Yes.

12 Q. So is it conceivable, therefore, that WikiLeaks could track
13 the March 2, March 3 version from a much later backup?

14 A. It's a possibility, yes.

15 Q. And is that true also through Confluence?

16 A. Yes, it's a possibility.

17 Q. OK. So the WikiLeaks materials did not have to come from
18 the 3/3 backup delivered to it; it could have come from a later
19 version stored on the Altabackups, correct?

20 A. It's a possibility, yes.

21 MR. BRANDEN: Judge, how are we doing now?

22 THE COURT: You're doing much better, Mr. Branden.

23 We'll break for lunch.

24 MR. BRANDEN: I appreciate it. Thank you.

25 (Continued on next page)

K2dWsch4

1 (Jury not present)

2 THE COURT: You're on cross-examination now,
3 Mr. Berger, so don't talk to anybody on the government team.

4 THE WITNESS: OK.

5 THE COURT: Thank you.

6 See you at 1:30.

7 (Luncheon recess)

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

K2D3SCH5

Berger - Cross

AFTERNOON SESSION

1:45 p.m.

(In open court; jury present)

THE COURT: Mr. Berger?

All right, Mr. Branden.

BY MR. BRANDEN:

Q. Mr. Berger, in your slide presentation around slide 37 -- but I don't need it -- you testified a bit about the Tor, correct?

A. Correct.

Q. And what does Tor stand for?

A. I believe it stands for The Onion Router.

Q. Do you know when it was created or where it was created?

A. I believe it was created at least 15 years ago or so by some entity of the U.S. government, I'm not sure which part.

Q. Okay. Do you know where it gets its funding?

A. I'm not sure, no.

Q. Do you know whether organizations like Facebook offer an Onion variance, a way to communicate through Onion?

A. I don't know specifically about Facebook. I do know that there are several organizations that offer a dot onion URL to connect to their services.

Q. People would want that facility to protect their privacy, correct?

A. Yes.

K2D3SCH5

Berger - Cross

1 Q. Do you know generally whether Tor is used by privacy
2 advocates in general?

3 A. I believe it is.

4 Q. Are you familiar with the Electronic Frontier Foundation?

5 A. I've heard of them, yes.

6 Q. Do you know whether they support the use of Tor?

7 A. I don't.

8 Q. You also testified about encrypted containers, correct?

9 A. Correct.

10 Q. Are there major vendors that support the use of encrypted
11 containers, so for example, does Microsoft produce such a
12 device?

13 A. They produce software that enables encryption, yes.

14 Q. What about Apple; also?

15 A. Yes.

16 Q. So there's nothing inherently nefarious or sinister about
17 the use of such a container, correct?

18 A. Yes, correct.

19 Q. In essence what it does, it allows the user to protect the
20 data from inspection by third parties; is that right?

21 A. Yes.

22 Q. So for example, if I have a home computer and it's going on
23 the fritz, if I had put my vital statistics into an encrypted
24 container, the repairer won't be able to get to that stuff; is
25 that correct, for example?

K2D3SCH5

Berger - Cross

1 A. Essentially, yes.

2 Q. You testified as to evidence that the defendant himself had
3 downloaded an encrypted container on April 18, correct?

4 A. Downloaded an encrypted container?

5 Q. Yeah.

6 A. I --

7 Q. Used an encrypted container?

8 A. I believe I testified that he used an encrypted container,
9 yes.

10 Q. Yeah. Did you look through his prior history before
11 April 18 to see whether he had used such a container earlier?

12 A. I believe there was -- I believe there was evidence of it
13 being used prior to that date. I can't confirm that, no.

14 Q. You also testified about Tails, correct?

15 A. Yes.

16 Q. Okay. Can you tell me again what Tails is.

17 A. So, Tails is a operating system that is designed to boot
18 off of a piece of removable media such as a DVD or a USB drive.
19 The entire operating system is loaded into memory. It doesn't
20 touch the hard drive. And its main purpose is to direct all
21 the network traffic, so anything you might be doing in your web
22 browser, over the Tor network.

23 Q. Part of Mr. Schulte's job at the CIA involved collecting
24 data stored on enemy computers; is that correct? Would you say
25 that's fair?

K2D3SCH5

Berger - Cross

1 A. From what I understand, yes.

2 Q. So given that that's part of his job description, would it
3 have been part of his work interest in operating a system that
4 had no persistent data, like Tails would allow?

5 A. It's possible.

6 Q. On slide 46, please. This item here in the middle section
7 of this slide, this has multiple ports, does it not?

8 A. Multiple ports for hard drives or other ports?

9 Q. Tell me what this device would do.

10 A. So, it allows you to connect two different hard drives to
11 your computer.

12 Q. Okay. What's the capacity of these hard drive, how much
13 does it hold?

14 A. Depends on what hard drives you put into the at adapter.
15 The adapter itself doesn't have capacity.

16 Q. I see. Okay. I think you testified on direct that the
17 defendant's home computer was configured to use RAID; is that
18 correct?

19 A. Correct.

20 Q. Given that, wouldn't it be necessary to wipe the disc clean
21 first to use that function?

22 A. To use what function?

23 Q. RAID.

24 A. You are you asking if you need to wipe a hard drive prior
25 to setting up a RAID?

K2D3SCH5

Berger - Cross

1 Q. Yeah.

2 A. Generally when you set up a RAID array, it will delete
3 whatever was on there. The RAID initiation process would
4 render any data on the drives previously unusable.

5 Q. So it would be important to clean those drives beforehand
6 if you wanted to save that data, for example, correct?

7 A. Correct.

8 Q. Are you aware that the defendant had a large movie
9 collection?

10 A. I have been informed of that, yes.

11 Q. Okay. And in the defendant's New York apartment, he had a
12 large amount of computer ware, did he not?

13 A. Yes.

14 Q. Did he have a lot of capacity to store these movies?

15 A. From what I understand, yes.

16 Q. With regard to Eraser Portable that you testified again,
17 please tell me what that is.

18 A. That is a utility designed to securely erase files and
19 folders.

20 Q. Does that leave a log of the folders that you've erased?

21 A. It depends on how you use the program.

22 Q. It can leave a log, correct?

23 A. It leaves artifacts based on how you use the program.

24 Certain operations of the program will leave certain artifacts.

25 Q. Does it always leave these artifacts?

K2D3SCH5

Berger - Cross

1 A. Again, the artifacts are dependent on what operations you
2 use the program for.

3 Q. So, if you wanted to cover your tracks totally, maybe
4 Eraser Portable wouldn't be the way to go, correct?

5 A. It's possible, yes.

6 Q. Slide 55, please, then 56. So these are the two folders
7 that Mr. Schulte deleted; is that correct?

8 A. Correct.

9 Q. As far as this investigation goes, you've heard the phrase
10 Brutal Kangaroo, correct?

11 A. Yes.

12 Q. But as to the home folder Brutal Kangaroo, you really don't
13 have any idea what was in that folder; is that correct?

14 A. You mean the folder that this is referring to on the D
15 drive, the Brutal Kangaroo folder?

16 Q. Yeah.

17 A. No, I do not know what was in there.

18 Q. As to array list. Have you heard that term before?

19 A. Yes, I have.

20 Q. Okay. Have you only heard that term as part of this
21 investigation?

22 A. No, I have not.

23 Q. What is array list?

24 A. It's a data structure used in the field of computer
25 science.

K2D3SCH5

Berger - Cross

1 Q. You don't know necessarily, even though the folder is
2 called "array list," whether it contained array list, correct?

3 A. That's correct.

4 Q. Furthermore, the title, the words "Brutal Kangaroo," you
5 don't know those two words in combination to be classified, do
6 you?

7 A. I believe they were classified. I don't know for sure.

8 Q. You don't know for sure. Okay. Would it be possible for
9 somebody like Mr. Schulte to be working on some aspect of
10 Brutal Kangaroo from his home and then bring it into the
11 office?

12 A. It would be possible, yes. I don't know procedurally if
13 that's allowed, but from a technical standpoint you can bring
14 data from one computer to another.

15 Q. And then once that information is safely within the CIA, it
16 would be important for him to delete the home version of that
17 folder, perhaps?

18 A. If that's what he wanted to do, yes.

19 Q. You also testified about the deletion of data and the
20 confirmation of transferred data, correct?

21 A. I believe you're referring to the Google searches?

22 Q. Yeah.

23 A. Yes.

24 Q. Okay. And again, deleting files, there's nothing sinister
25 about doing that?

K2D3SCH5

Berger - Cross

1 A. Just generally deleting files, depends on what the files
2 are, but yes.

3 Q. And wiping a drive clean is a common procedure for most
4 people; is that correct?

5 A. I wouldn't say most people. It depends on the type of
6 user.

7 Q. Okay. And you testified about the use of DBAN. Correct?

8 A. Yes.

9 Q. And are you familiar with the fact that Best Buy and
10 Staples recommend DBAN before disposing of a disc?

11 A. I'm not familiar with that, no.

12 Q. Are you familiar with the -- are you aware that MacOS has a
13 disc wipe option?

14 A. Yes, I am.

15 Q. Okay. Window also has a disc wipe option, correct?

16 A. Correct.

17 Q. With regard to slides 70 and 71, please. I think you
18 described 70 and 71 as evidence that the defendant had
19 reformatted his computer, correct?

20 A. Correct.

21 Q. Do you know if this was definitely a reformatting or is the
22 defendant just upgrading hardware and installing new file
23 systems?

24 A. You wouldn't upgrade your file system when you're
25 installing new hardware. This is a reformat because it shows a

K2D3SCH5

Berger - Cross

1 creation of the MFT. This -- the MFT is the underlying basis
2 for your file system. Even if you were to upgrade to a newer
3 version of Windows, let's say, that would not create a new MFT.
4 The only thing that would trigger the creation of a new MFT
5 would be reformatting the system.

6 Q. Throughout -- you see we're getting near the end of these
7 slides, so I have some general followup questions for you.

8 Throughout your investigation, have you found any evidence
9 that the defendant copied the Vault 7 or 8 data on to his home
10 computer?

11 A. Not directly, no.

12 Q. Okay. Have you found any evidence that the defendant
13 brought hard drives home from the CIA?

14 A. No.

15 Q. Have you found any evidence that the defendant plugged any
16 hard drives from the CIA into his home computer?

17 A. No.

18 Q. Do you have any evidence that the defendant ever took data
19 from the CIA home to put it into his home computer?

20 Essentially the same question, again.

21 A. No.

22 Q. Do you have any evidence that the defendant stored
23 Confluence on his home computer?

24 A. No.

25 Q. How about Stash?

K2D3SCH5

Berger - Cross

1 A. No.

2 Q. Or the Atlassian suite, for example?

3 A. No.

4 Q. Do you have any evidence that Altabackups was stored on his
5 home computer?

6 A. No.

7 Q. Do you have any evidence that the Confluence backup
8 accessed allegedly on 4/20 was ever stored on the defendant's
9 home computer?

10 A. No.

11 Q. Then finally I have one question that's just something of a
12 hypothetical. But, mostly you testified with regard to the
13 home computer stuff, those dates concerned April and May of
14 2016. Correct?

15 A. Correct.

16 Q. Okay. Did you become aware that the defendant left the CIA
17 at some point?

18 A. Yes.

19 Q. Do you know when that was?

20 A. I believe approximately October, November of 2016.

21 Q. Did he relocate?

22 A. Yes, I believe he did.

23 Q. Where did he move to?

24 A. He moved to New York.

25 Q. And did he get a new job?

K2D3SCH5

Berger - Redirect

1 A. Yes.

2 Q. Okay. And when was the search of his New York apartment?

3 A. It was some time in March of 2017 I believe.

4 Q. Is it your suggestion that the devices from his home that
5 you searched and analyzed are the same devices that he had in
6 Virginia, a year earlier?

7 A. The devices were found in the defendant's apartment.

8 Q. Okay. If someone had something really terrible in their
9 devices in their home computer, and they were moving to a whole
10 other place, would it have been more advisable to just destroy
11 that home computer and all removable media, and buy new stuff
12 when you get to New York? Would that have been a safer, more
13 prudent thing to do?

14 A. If they had reason to believe that there was evidence of
15 that on those drives, sure.

16 MR. BRANDEN: That's all I have, Judge.

17 THE COURT: Mr. Kamaraju.

18 MR. KAMARAJU: Just a few questions, your Honor.

19 REDIRECT EXAMINATION

20 BY MR. KAMARAJU:

21 Q. Do you remember Mr. Branden asked you about whether you
22 reviewed the entire leak page by page?

23 A. Yes.

24 Q. He asked you some questions about reviewing two data
25 points?

K2D3SCH5

Berger - Redirect

1 A. Yes.

2 Q. To arrive at your ultimate conclusion, did you only look at
3 two data points?

4 A. No.

5 Q. Did you do any analysis of the rest of the leak?

6 A. Yes.

7 Q. Can you describe for the jury what you did.

8 A. So, we looked at several data points. We looked at pages
9 that were in the leak and we looked at their corresponding
10 records in the database. We found that there was a -- it
11 started to form a pattern. There were data that was in the
12 database that was on WikiLeaks, and there was data in the
13 database not present on WikiLeaks.

14 We then looked at the distance between those points,
15 and then we started to move to points that were closer and
16 closer together. We then arrived at a set of two points for
17 each system, Atlassian, the Atlassian Confluence product and
18 the Stash product. We picked the two points that were closest
19 together from either side of the line. The line being the
20 division between data from the databases that was on WikiLeaks,
21 and data that was not on WikiLeaks.

22 Q. Did you do anything to determine whether there was any data
23 released by WikiLeaks that came after March 3, 2016?

24 A. Yes, we did.

25 Q. Can you describe for the jury what you did.

K2D3SCH5

Berger - Redirect

1 A. One of the things that we did was look through the content
2 of the pages that was present on WikiLeaks, and we searched the
3 text of those pages for dates in different formats.

4 You can have a date that is a two-day month, two-day
5 day and a four-day year. You could have a date format that
6 starts with a four-day year, then the month and the day. Two
7 digit year. So there is several variations of how people
8 document dates.

9 We looked at several of those and ran searches for
10 dates with the year 2016, 2017, through the WikiLeaks data.

11 Q. After you did that, is your opinion still that the data
12 comes from the March 3, 2016, time period?

13 A. Yes, it is.

14 Q. You remember Mr. Branden asked you about whether it was
15 also possible that data came from a later backup; do you
16 remember that?

17 A. Yes.

18 Q. You said it was a possibility, right?

19 A. Yes.

20 Q. Do you think that's what happened here?

21 A. No, I don't.

22 Q. Why not?

23 A. Two primary reasons. Number one, Mr. Leedom testified
24 yesterday about what the reconstruction process would have been
25 like if you had taken the backup from Confluence and tried to

K2D3SCH5

Berger - Redirect

1 reconstruct pages that were displayed on WikiLeaks. He also
2 explained how due to an error with the backup script, there was
3 corruption in parts of the Confluence database that would have
4 made it exceedingly difficult to reconstruct everything.

5 If you wanted to go and take that data and then roll
6 it back to earlier versions to make it, let's say, look like a
7 previous version, that would have been another added layer of
8 complexity on an already hard process.

9 The second reason is my understanding of how WikiLeaks
10 works, which is they like to publish lots of data. If they had
11 data in their possession from a later date, and only released
12 data up to a previous point in time, that would mean that in
13 their possession they have that additional data that they have
14 not put out.

15 Q. Do you remember you were asked about whether you knew what
16 was in the Brutal Kangaroo and array list folders on the
17 defendant's computer?

18 A. Yes.

19 Q. When you looked at the forensic image of the defendant's
20 home computer network, could you access those folders?

21 A. No.

22 Q. Why not?

23 A. Because they had been deleted.

24 Q. What had they been deleted with?

25 A. Eraser Portable.

K2D3SCH5

Berger - Redirect

1 Q. Does that mean they were securely erased?

2 A. Yes, it does.

3 Q. You were also asked a series of questions about whether you
4 found evidence of Confluence on the defendant's computer or the
5 Altabackups on the defendant's computer; do you remember that?

6 A. Yes.

7 Q. You remember testifying about the defendant reformatting
8 his computer?

9 A. Yes.

10 Q. What would that do to the data that was on his computer
11 prior to the reformat?

12 A. When you reformat, you wipe away the existing file system
13 and you build a new file system on top of that. Anything that
14 was there is now available to be overwritten. So over time,
15 files would get overwritten that were not part of the new file
16 system.

17 Q. Do you remember Mr. Branden asked you some questions about
18 the initial report that you put out?

19 A. Yes.

20 MR. KAMARAJU: Ms. Hurst, can we pull up Government
21 Exhibit 1207-27 and 30, please. For 1207-27, let's just blow
22 up the area around the government exhibit and header. I think
23 you've done a bunch before. Thank you.

24 Q. At the time of your initial report, had you seen Government
25 Exhibit 1207-27?

K2D3SCH5

Berger - Redirect

1 A. I had not.

2 MR. KAMARAJU: Can we do the same thing for 30,
3 please.

4 Q. How about 1207-30. At the time of your initial report had
5 you seen this exhibit?

6 A. I had not.

7 Q. Prior to your testimony, have you seen these exhibits?

8 A. Yes.

9 Q. Does Government Exhibit 1207-27 and 1207-30 change your
10 conclusion that the data on WikiLeaks was dated March 3, 2016?

11 A. No.

12 Q. What, if any, impact on your opinion do these two exhibits
13 have?

14 A. It confirms the results of the -- the data that's in the
15 report, and it allows me to draw an opinion that the data came
16 from that backup file, the March 3 backup file.

17 Q. Why is that?

18 A. Because the data in the backup file would fit within the
19 window that was defined in the report.

20 MR. KAMARAJU: One moment, your Honor. No further
21 questions your Honor.

22 THE COURT: You're excused. Thank you very much.

23 (Witness excused)

24 THE COURT: Call your next witness.

25 MR. LAROCHE: The government calls Bonnie Stith, your

K2D3SCH5

Stith - Direct

1 Honor.

2 THE DEPUTY CLERK: Please state your name for the
3 record.

4 THE WITNESS: Bonnie Bennett Stith.

5 (Witness sworn)

6 THE COURT: All right, Mr. Laroche.

7 MR. LAROCHE: Thank you, your Honor.

8 BONNIE BENNETT STITH,

9 called as a witness by the Government,

10 having been duly sworn, testified as follows:

11 DIRECT EXAMINATION

12 BY MR. LAROCHE:

13 Q. Good afternoon, Ms. Stith.

14 A. Good afternoon.

15 Q. Have you worked at the CIA?

16 A. I have.

17 Q. For approximately how long did you work at the CIA?

18 A. 34 years.

19 Q. Do you work there anymore?

20 A. I do not.

21 Q. Why don't you work there anymore?

22 A. I retired.

23 Q. When did you retire?

24 A. I retired the 3rd of January, 2017.

25 Q. Prior to your retirement, what was your position within the

K2D3SCH5

Stith - Direct

1 CIA?

2 A. Immediately prior to my retirement, I was the director for
3 the Center for Cyber Intelligence.

4 Q. When did you become the director of the Center for Cyber
5 Intelligence?

6 A. September 2015.

7 Q. Does that go by CCI?

8 A. Yes, it does now. It was Information Operations Center at
9 the time.

10 Q. What is CCI?

11 A. CCI is the Center for Cyber Intelligence. It is the -- I
12 would say the premier cyber collection organization of the U.S.
13 government, but certainly of the CIA.

14 Q. Is the director position the highest ranking position
15 within CCI?

16 A. It is.

17 Q. Generally, what were your responsibilities as director of
18 CCI?

19 A. My general responsibilities were to set the vision,
20 establish priorities, oversee the progress towards collecting
21 better intelligence faster, and managing up and out towards
22 modernization, which was a reorganization going on at the
23 agency.

24 Q. When you were director of CCI, approximately how many
25 employees did you oversee?

K2D3SCH5

Stith - Direct

1 A. Several thousand.

2 MR. LAROCHE: Can we bring up Government Exhibit 89,
3 please.

4 Q. You see CCI at the top of this exhibit?

5 A. Yes.

6 Q. There is the Engineering Development Group below that; do
7 you see that?

8 A. Yes.

9 Q. Was that the only group that you oversaw?

10 A. No.

11 Q. Approximately how many other groups did you oversee?

12 A. In excess of 14.

13 Q. Are you familiar with the position developer?

14 A. Yes, I am.

15 Q. Just generally, what is a developer?

16 A. They write code to help us develop the capabilities to
17 access cyber means to get to intelligence.

18 Q. About how many levels of management were between you and a
19 developer?

20 A. Could have been six, could have been seven, could have been
21 eight.

22 Q. How many times as director of CCI did you deal with a
23 dispute among developers?

24 A. Only once.

25 MR. LAROCHE: We can pull that exhibit down.

K2D3SCH5

Stith - Direct

1 Q. Who was that dispute between?

2 A. It was between Amol and Josh.

3 Q. Josh --

4 A. Josh Schulte.

5 Q. Did you become aware of that dispute in about March 2016?

6 A. Yes, I did.

7 Q. Prior to that time, had you any interactions with those
8 individuals?

9 A. I don't recall ever interacting before that time.

10 Q. How did you learn about the dispute between them?

11 A. I learned that there had been an exchange of words between
12 a couple of developers that I viewed as unprofessional
13 behavior, and it had resulted in some disruption in that
14 branch.

15 Q. After learning of that dispute, did you meet with the
16 defendant and Amol?

17 A. I did.

18 Q. Did you meet with them separately or together?

19 A. Together.

20 Q. At the time, did you have an understanding that the
21 defendant had alleged that Amol threatened him?

22 A. I did.

23 Q. Why did you decide to have the meeting together?

24 A. It had been investigated by the threat management unit, and
25 I had talked to the leadership involved, and there didn't seem

K2D3SCH5

Stith - Direct

1 to be any foundation to that.

2 Q. Approximately when did the meeting occur?

3 A. It would have been in March. Some time after that.

4 Q. Did you have any difficulty getting the defendant and Amol
5 to come to that meeting?

6 A. I did.

7 Q. What was the difficulty?

8 A. Josh did not want to meet with Amol. He said that he was
9 afraid of Amol, and that he didn't want to be in the same room
10 meeting with him.

11 Q. Did he come to the meeting?

12 A. He did.

13 Q. Why?

14 A. Because I insisted.

15 Q. During the meeting, what, if anything, did you say to them?

16 A. The meeting was really about me telling them what I
17 expected of them as employees of the U.S. government, as
18 employees of the agency, and as really, what I considered to be
19 stewards of the public trust in the space that we were in.

20 I talked to them about responsibility for what they
21 were supposed to be doing, about the honor that we had as
22 people that got to work for the agency, and about the
23 obligation that we had to our nation.

24 (Continued on next page)

K2dWsch6

Stith - Direct

1 MS. SHROFF: I'm sorry. I missed the last part.

2 THE WITNESS: The obligation that we had to our
3 nation.

4 MS. SHROFF: Thank you.

5 BY MR. LAROCHE:

6 Q. How did Amol react to that?

7 A. Amol, I think, was chagrined at having to be there. He
8 seemed -- I don't -- it wasn't usual for a developer to come
9 before the director in that space, so I think he was
10 embarrassed.

11 Q. What about the defendant?

12 A. Josh didn't really exhibit much emotion.

13 Q. Do you recall whether the defendant said anything during
14 that meeting?

15 A. I don't recall.

16 Q. After you met with the defendant and Amol, were they moved
17 within their branch?

18 A. Yes.

19 Q. Were you consulted on that decision?

20 A. I don't recall directly, but probably.

21 Q. And why do you say that?

22 A. I think we had made the decision at that point that they
23 needed to be separated, so --

24 Q. Why?

25 A. We needed the work to continue, and if they couldn't

K2dWsch6

Stith - Direct

1 continue working in the same space, then they needed to be
2 separated so they could continue to work.

3 Q. And why did you need the work to continue?

4 A. The motto of the Center for Cyber Intelligence is "we can
5 produce better intelligence faster." Our nation depended on us
6 to do that, and we had important work going on. And at the
7 very foundation of the cyber effort is the code writing and the
8 tool development that goes on, and I needed them to be focused
9 on that job.

10 Q. Now, did there come a time when you learned that the
11 defendant had filed a protective order against Amol?

12 A. I was briefed on that, yes.

13 Q. In your experience at the CIA, are you aware of another
14 time where that's happened between two agency employees?

15 A. No.

16 Q. What, if any, action was taken as a result of that
17 protective order?

18 A. I think at that point -- well, we called in threat
19 management unit again. We also called in security because it
20 was, it was so unusual to have agency employees in a local
21 court for those issues that there was another investigation
22 that was, I think, started. But also, I think we then
23 separated them even further.

24 MR. LAROCHE: Could we pull up Government Exhibit
25 1046, please, and go to the second page. And just zoom in on

K2dWsch6

Stith - Direct

1 the bottom email, please.

2 Q. Who sent this email?

3 A. Deborah.

4 Q. And who did she send it to?

5 A. She sent it to Amol and Josh.

6 Q. And why did she send this email?

7 A. To inform them they would be moving into different
8 cubicles.

9 MR. LAROCHE: Let's go up to the next email. Maybe
10 just go up one more slide and see who sent it.

11 Q. This is on March 29, is that correct?

12 A. Uh-huh.

13 Q. Who sends this email?

14 A. Anthony.

15 Q. And who did he send it to?

16 A. He sent it to Amol and Josh and carbon copied Michele,
17 Susan and Dana.

18 MR. LAROCHE: Let's go to the next slide.

19 Q. Are you copied on this email?

20 A. I am.

21 Q. Who else is copied?

22 A. John, Karen, Michael, Anthony, Deborah and Sean.

23 Q. Do you see in the first sentence it says, "After further
24 consultations with HR, security and the CC front office"?

25 A. The CCI front office, yes.

K2dWsch6

Stith - Direct

1 Q. Do you have an understanding of what that's referring to?

2 A. We had a meeting to discuss what was going on, and a
3 decision was made that they would be separated.

4 Q. Why is that?

5 A. At that point I think there was a restraining order
6 granted, and so, in order to continue working, we wanted them
7 in different places.

8 I also did not believe that one should be moved and not the
9 other. Because it was unclear as to really what was going on,
10 I thought both of them should be moved.

11 MR. LAROCHE: Let's go to the next email, please.
12 Just zoom in on that, please.

13 Q. We're still on March 29, is that correct?

14 A. Yes.

15 Q. Who sent this email?

16 A. Anthony.

17 Q. Sorry. At the top there, on the "from"?

18 A. Oh, I'm sorry. It was from Josh.

19 Q. That's OK.

20 A. It was to Anthony.

21 Q. And did he copy all the same folks as before?

22 A. Yes.

23 Q. And do you see that on the copy line, and this person was
24 on the last email, is Karen?

25 A. Yes.

K2dWsch6

Stith - Direct

1 Q. Who is Karen?

2 A. Karen -- that was Karen. She is the group chief.

3 Q. And if we could just read that sentence, please?

4 A. "I just want to confirm this punishment of removal from my
5 current branch is for reporting to security an incident in
6 which my life was threatened and/or for resubmitting a
7 protective order against Amol."

8 Q. And you said you were involved in those consultations about
9 the move, is that correct?

10 A. Yes.

11 Q. Was that move punishment?

12 A. No.

13 Q. Why not?

14 A. Based on what was going on, we felt it was in everybody's
15 best interests to have them separated, and if we were going to
16 move one, it seemed the other should be moved as well. And
17 since there was no clear-cut case for what was going on, we
18 opted to move them both.

19 MR. LAROCHE: Let's go to the next email.

20 Q. And this is still on March 29, is that correct?

21 A. Yes.

22 Q. And who sent this email?

23 A. It was Josh.

24 Q. Did you receive this email?

25 A. I did.

K2dWsch6

Stith - Direct

1 Q. If you can just read the first two sentences, please.

2 A. "I was told that there would be no written response to my
3 email, so I'm proceeding with my move, assuming it is directly
4 due to with my security report."

5 Q. Did you tell the defendant that there would be no written
6 response to his email?

7 A. No.

8 Q. Are you aware of anyone else telling him that?

9 A. No.

10 MR. LAROCHE: We can pull that down.

11 Q. Now, after this email exchange, did there come a time when
12 you learned about a hearing related to the protective order
13 between Josh and Amol?

14 A. Yes.

15 MR. LAROCHE: Let's pull up Government Exhibit 1051,
16 please, and if we can just look at the bottom.

17 Q. Do you see there's an email dated April 6, 2016, at 3:35?
18 This is at the far bottom.

19 A. At the far bottom, yes.

20 Q. Is that an email from Josh?

21 A. Yes, it is.

22 MR. LAROCHE: Let's go to the next slide, please.

23 Q. And just who did Josh send this email to?

24 A. He sent it to Michele, to Susan, to me, to Michael and to
25 William.

K2dWsch6

Stith - Direct

1 Q. Now, had you reviewed this email before your testimony
2 today?

3 A. Yes.

4 Q. And just generally, what does the defendant address in this
5 email?

6 A. The protective order that he had filed against Amol.

7 Q. Was it typical for you to receive emails like this from
8 developers?

9 A. No.

10 Q. How many emails like this did you receive from developers
11 while you were director of CCI?

12 A. Only from Josh.

13 Q. Can you go to the first sentence of this -- I'm sorry.
14 Read the first sentence.

15 A. "Today was the hearing for the protective order I filed
16 against Amol."

17 Q. Were you present at that hearing?

18 A. No, I was not.

19 Q. Are you aware of what happened at that hearing?

20 A. No.

21 MR. LAROCHE: Let's go to the, zoom in on the second
22 paragraph, please.

23 Q. See where there's a reference to EAP?

24 A. Yes.

25 Q. Just generally, what is EAP?

K2dWsch6

Stith - Direct

1 A. EAP is the agency's employee assistance program. We have
2 psychologists. We have financial counselors. There's all
3 kinds of resources for people that are having issues going on
4 of any type, and so, it is a resource for agency employees.
5 They can self-refer or otherwise.

6 Q. Do you see the sentence starting "therefore," the second
7 from the bottom?

8 A. "Therefore," yes.

9 Q. Can you read that?

10 A. "Therefore, someone in my management chain clearly told
11 Amol about my second appointment."

12 Q. And just read it to the end.

13 A. "Why? Why is information that I thought confidential being
14 shared with Amol?"

15 Q. Did you share any information about EAP with Amol?

16 A. No.

17 Q. Are you aware whether or not anyone else did?

18 A. No.

19 MR. LAROCHE: If we can zoom out again and zoom in on
20 the paragraph starting Bonnie.

21 Q. Let's just read the first sentence, please?

22 A. "Bonnie, I'm very concerned with EDG and chief EDG's
23 handling of this incident, and I'm hoping you can help me."

24 Q. Just pause there for a second. You see the C forward slash
25 EDG; do you have an understanding of who that refers to?

K2dWsch6

Stith - Direct

1 A. Karen.

2 MS. SHROFF: I'm sorry?

3 MR. LAROCHE: I believe the witness said Karen.

4 Q. Is that correct?

5 A. Yeah, it would have been Karen, the chief of EDG.

6 Q. Let's continue reading from the "I know you don't."

7 A. "I know you don't want to be involved with this, and I'm

8 sorry it took place under your management. But I am running

9 out of upper management and HR people to inform. From the

10 onset of this entire situation, I have only wanted to be taken

11 seriously and treated fairly, neither of which has happened."

12 Q. Do you agree that he wasn't taken seriously with respect to

13 this complaint?

14 A. No.

15 Q. Why don't you agree with that?

16 A. The fact that I met with him; the fact that I was being

17 briefed on them; the fact that this was an ongoing situation.

18 We were all taking it very seriously. We had threat management

19 unit involved. We had security involved. People were looking

20 into this to make sure that there wasn't something else going

21 on.

22 MR. LAROCHE: We can zoom out and go to the next

23 paragraph, please.

24 Q. And just read the first sentence.

25 A. "My life was threatened by Amol, and I seriously felt he

K2dWsch6

Stith - Direct

1 may kill me or others."

2 Q. As director of CCI, what steps would you have taken if you
3 believed someone was going to kill someone at CCI?

4 A. They wouldn't have been at work.

5 Q. Did you take those steps with respect to Amol?

6 A. No.

7 Q. Why not?

8 A. We had an investigation, and the investigation did not
9 merit that.

10 Q. If we can go to the last sentence that starts "despite."

11 A. OK. "Despite Amol admitting his actions on 3/1 to
12 security, I felt that the issue still wasn't taken seriously."

13 Q. Do you have an understanding of what he's referring to by
14 "admitting his actions on 3/1 to security"?

15 A. No.

16 MR. LAROCHE: If we can go to the next line at the
17 bottom.

18 Q. Just read that sentence, please.

19 A. "From the time I reported the incident, chief EDG has still
20 never sat down and talked to me."

21 Q. Again, who is that a reference to?

22 A. Karen.

23 MR. LAROCHE: Let's go to the next page, please, and
24 just zoom in on the top paragraph.

25 Q. Just continue reading the end of that sentence.

K2dWsch6

Stith - Direct

1 A. "Was no discussion of safety in the workplace or my
2 concerns of working directly with Amol."

3 Q. And then the next sentence.

4 A. "I was told to go back to work, and despite my concerns to
5 management of working next to Amol, I was told there were no
6 seats to move us."

7 Q. Did you tell the defendant to go back to work during your
8 meeting?

9 A. No -- well, yes, I did tell him to go back to work.

10 Q. Why?

11 A. Because what we do is important. And again, there had been
12 no indication that there was a real threat there. My feeling
13 was go back to work and focus on what's important.

14 MR. LAROCHE: Let's zoom out again.

15 Go to the next paragraph, please.

16 Q. Do you see there's a sentence that starts -- sorry. Read
17 until the "my management" in the second line.

18 A. "At some point I sat down directly with you, Bonnie. You
19 told me I didn't have to worry about losing my job over this.
20 Perhaps you can see my frustration in all this. My management,
21 specifically Karen, has fundamentally failed to ensure my own
22 safety, and now I feel my management is informing Amol of
23 information that he does not need to know. I'm very upset with
24 all of this and feel that management's only concern is CYA and
25 not their employees."

K2dWsch6

Stith - Direct

1 Q. Did you agree with the assertion that Karen had failed to
2 ensure the defendant's safety?

3 A. No.

4 Q. Why not?

5 A. Again, we'd called in security. People had been
6 interviewed. There'd been an investigation of what was going
7 on, and there was nothing found.

8 Q. And did you agree with the assertion that management's only
9 concern was CYA?

10 A. No.

11 Q. Finally, can you please read the last paragraph.

12 MR. LAROCHE: We can zoom out and then zoom in.

13 A. "More than anything, I want this situation to go away. But
14 as I still feel I'm being punished and my management does not
15 have my back and that confidential information is told to Amol,
16 how can I feel any level of trust from my management? I
17 sincerely hope you can assist me."

18 Q. Did you respond to this email?

19 A. I believe I did.

20 MR. LAROCHE: Let's take a look at the response on the
21 first page. If you could just zoom in on that, please.

22 Q. When did you send this response?

23 A. April 6 at 7:27 p.m.

24 Q. Is that the same day you got the email?

25 A. I think it would have been.

K2dWsch6

Stith - Direct

1 MR. LAROCHE: We can just zoom out and show you the
2 bottom.

3 A. Yeah. OK.

4 Q. Could you please summarize what you said in response?

5 A. I told Josh I'd seen his note and I had read it, and I
6 wanted to reassure him that we were taking it very seriously.
7 And to my knowledge, no confidential information had been
8 shared with anybody regarding any appointments or conversations
9 that anyone had had with EAP.

10 Q. You testified that you disagreed with some of the things
11 that the defendant said in his email to you?

12 A. Yes.

13 Q. Why didn't you address those in response?

14 A. They weren't worth addressing. What I wanted was for him
15 to focus on what was supposed to be the most important thing
16 going and off the rest of this stuff. It seemed like there was
17 a constant distraction going on.

18 MR. LAROCHE: Let's just zoom back out and then zoom
19 in on the defendant's response.

20 Q. Do you see you received this the next day, on April 7? Is
21 that right?

22 A. Yes.

23 Q. Can you please read what the defendant said in response.

24 A. "Thank you. I'm hoping to focus on the Vortex and other
25 tool rewrites for the remainder of the week and ignore all the

K2dWsch6

Stith - Direct

1 rest of the noise."

2 Q. What was your reaction to that?

3 A. I was relieved.

4 Q. And why?

5 A. I was writing notes at 7:56 at night. My day went from
6 about 8:00 to about 5:00 with back-to-back meetings, and with
7 everything else going on, this was a lot. I mean, I felt for
8 what was happening here, but there was a lot of other stuff
9 going on. I wanted Josh to settle down and get to work.

10 Q. Was that the last time you became aware of a problem with
11 the defendant?

12 A. I don't recall.

13 Q. Did you later learn about issues with the defendant's
14 privileges to a computer system?

15 A. Yes.

16 Q. And how did you learn about that?

17 A. I was briefed. They had switched jobs. And when you
18 switch a job at the agency, typically you lose access to the
19 things you were doing before and they move you to another
20 project and grant you accesses to that project. What was
21 happening was that Josh was going back and recreating his
22 accesses back into the area he was before.

23 Q. Now, did you have any involvement in dealing with those
24 issues?

25 A. Other than being briefed and making sure that they were

K2dWsch6

Stith - Direct

1 being documented, no.

2 Q. And who was principally responsible, generally, for dealing
3 with those activities?

4 A. At that point it was Mike.

5 MS. SHROFF: I'm sorry?

6 THE WITNESS: Mike.

7 BY MR. LAROCHE:

8 Q. And was he part of management?

9 A. He was. At that point I think he was the acting chief.

10 Q. Of what part?

11 A. Of EDG.

12 Q. Of EDG?

13 A. Uh-huh.

14 Q. Now, earlier you said that one of the things you conveyed
15 was you wanted Amol and the defendant to just get back to work,
16 is that right?

17 A. Yes.

18 Q. Why did you want them to do that?

19 A. Back to the responsibility we have to the public that's
20 paying us to keep them safe. And again, we've created a
21 culture in the organization that was really about moving
22 forward in an innovative way. This kind of nonsense got in the
23 way of a working environment for their colleagues and for the
24 rest of us, so we needed that job done.

25 Q. And what would happen if developers weren't able to do

K2dWsch6

Stith - Cross

1 their jobs?

2 A. Well, they probably shouldn't call us the cyber center
3 anymore. We had to be something else, because that was a key
4 piece of what went on in that organization.

5 Q. What impact would that have had on your mission?

6 A. We wouldn't have been able to complete our mission.

7 MR. LAROCHE: No further questions, your Honor.

8 THE COURT: Ms. Shroff.

9 CROSS-EXAMINATION

10 BY MS. SHROFF:

11 Q. Did you say the culture of the mission was to be moving
12 forward in an innovative way?

13 A. Yes.

14 Q. How many levels removed were you from EDG?

15 A. EDG was one of the groups that I supervised and led.

16 Q. And how many groups did you lead?

17 A. More than 14.

18 Q. And in more than 14 groups, were you aware that in this
19 particular group, grown men flicked rubber bands at each other?

20 A. At the end of the day --

21 Q. Just during the time it was going on, not --

22 A. No, I was not.

23 Q. OK. Were you aware that grown men had Nerf guns and were
24 shooting at each other?

25 A. No.

K2dWsch6

Stith - Cross

1 Q. Were you even aware that in one of your 14 branches there
2 were grown men with Nerf guns? Not one grown man, grown men.

3 A. It was a group. No.

4 Q. Were you aware that there were people shoving each other
5 into desks?

6 A. No.

7 Q. Were you aware there were people hitting each other? Grown
8 men, men of the age of 30, hitting each other.

9 A. No.

10 Q. Wasn't that the culture of EDG that you were completely
11 unaware of in April of 2016?

12 A. Yes.

13 Q. Right.

14 And who supervised these grown men?

15 A. Chief EDG.

16 Q. And who, pray tell, was chief EDG?

17 A. Karen.

18 Q. And she was responsible for supervising these individuals,
19 correct?

20 A. Karen was the group chief.

21 Q. Was she in charge of supervising them, ma'am?

22 A. She was their group chief.

23 MS. SHROFF: I'll take that as a yes.

24 Q. Did Karen ever come to you and say, I have these bunch of
25 grown men acting like this, help me?

K2dWsch6

Stith - Cross

1 A. No.

2 Q. Let me ask you a question. Was there an intermediary boss
3 between you and Karen?

4 A. No.

5 Q. Was there an intermediary boss between Karen and these EDG
6 developers?

7 A. Yes.

8 Q. And who, pray tell, was that?

9 A. There probably were a couple of levels. Sean was his
10 immediate boss.

11 Q. You had not a clue, did you, that any of this was going on
12 because Sean never, ever told anyone else? Correct?

13 A. I can't speak to that.

14 Q. Well, certainly you never heard from Karen that this was
15 going on, correct?

16 A. No.

17 Q. Would you say that the EDG group was an important group for
18 the CIA?

19 A. Yes.

20 Q. Tell them. Why was it important?

21 A. Those are the tool writers.

22 Q. Right.

23 A. They developed the capabilities.

24 Q. And they are the coders and the developers, correct?

25 A. Yes.

K2dWsch6

Stith - Cross

1 Q. And supervising them is an important job, correct?

2 A. Yes.

3 Q. As you said, it contributes to your mission, right?

4 A. Yes.

5 Q. And until one of the coders brought it to your attention,
6 you were clueless? Yes or no.

7 A. Yes.

8 Q. And it was, in fact, the coder that brought it to your
9 attention, right?

10 A. I don't recall him ever bringing that to my attention.

11 Q. Really? It wasn't Mr. Schulte who filed a complaint? He's
12 a coder, right?

13 A. The complaint wasn't about rubber bands and Nerf guns.

14 Q. I didn't ask you that. My question was, who brought on the
15 complaint?

16 A. Mr. Schulte filed a complaint --

17 Q. Right.

18 A. -- about --

19 Q. And Mr. Schulte filed a complaint about the way he was
20 being treated by Amol, correct?

21 A. Yes.

22 Q. And when he felt his complaint wasn't taken seriously, he
23 escalated it, right?

24 A. Yes.

25 Q. And nobody wanted it escalated, right? Well, Karen

K2dWsch6

Stith - Cross

1 certainly didn't want it escalated, right?

2 A. She never told me that.

3 Q. Well, did she escalate it?

4 A. I was briefed on it.

5 Q. No, no. That wasn't my question. Of course, you were
6 briefed on it. You were briefed on it because he wouldn't
7 stop, correct?

8 A. Yes.

9 Q. He kept escalating it. He escalated it, right?

10 A. He escalated it.

11 Q. Right. He felt he wasn't being treated fairly, correct?
12 Whether you agree with it or not, he felt his life was
13 threatened, correct?

14 A. Yes.

15 Q. He went and got a protective order in a courtroom, correct?
16 State courtroom, correct?

17 A. Yes.

18 Q. By the way, did you know at some point that people had
19 actually gone to court?

20 A. I was briefed on the fact that they had gone to court.

21 Q. Did somebody get a transcript and see what was said in that
22 proceeding?

23 A. It was handed to our security.

24 Q. OK. Let's go with that. Did security get you a
25 transcript?

K2dWsch6

Stith - Cross

1 A. No.

2 Q. You have two CIA employees going to a state court, correct?

3 A. Uh-huh.

4 Q. This is the last thing the CIA wants, am I right?

5 A. I don't know that I'd call it the last thing, but it's not
6 something that was done.

7 Q. I mean, isn't it fair to say no company wants that
8 headache? Right? Private, public, government, nobody wants
9 that, right?

10 A. I can't speak to that.

11 Q. OK. Well, you didn't want that, did you?

12 A. It wouldn't be my first choice, no.

13 Q. OK. And security was in charge of this, correct?

14 A. It was handed over to security.

15 Q. Right. Security never got you a copy of the transcript,
16 correct?

17 A. No.

18 Q. You have no idea what was even said by Amol in open court,
19 correct?

20 A. No.

21 Q. You have no idea if Amol actually told the judge that this
22 man has been sent to counseling, correct?

23 A. No.

24 Q. You do not know how Amol got that information, sitting here
25 to this day, correct?

K2dWsch6

Stith - Cross

1 A. No.

2 Q. And yet you think you knew the culture of EDG in April of
3 2016?

4 A. Yeah --

5 MS. SHROFF: I withdraw that.

6 Q. Let's just go back to the state complaint, shall we?

7 Did you, by any chance, ever find out how Amol knew he was
8 referred to therapy?

9 A. No.

10 Q. Did you ever try and tell Karen: Hey, you know, we may
11 want to find out why these two people who are at each other
12 know information that is upsetting to one developer, that is
13 personal to one developer, how does Amol know this? Did you
14 ever ask?

15 A. No.

16 Q. Do you recall a time when Karen ever tried to tell you how
17 Amol got that information?

18 A. No.

19 Q. Do you recall getting the Same Time chat or ping, whatever
20 it is that it's called, about Amol having information about
21 Mr. Schulte?

22 A. No.

23 Q. And it's fair to say that sitting here today you still
24 don't know how Amol got that information, right?

25 A. No.

K2dWsch6

Stith - Cross

1 Q. Now, you testified that there came a time that you sat down
2 and you had a meeting with these two individuals, right?

3 A. Yes.

4 Q. And is it fair to say that at the time you sat down with
5 them, you didn't really know whether they liked coding or they
6 didn't like coding? Right? Is that fair to say?

7 A. Yes.

8 Q. You just had these two problem people who were in your
9 office, right?

10 A. Yes.

11 Q. You did not know whether one, Amol, didn't mind if he was
12 no longer a coder, correct?

13 A. No.

14 Q. You didn't know if Amol's end goal in life was to be in
15 management and no longer be a coder, correct?

16 A. No.

17 Q. In fact, you didn't even know that Amol wanted to be in
18 management, correct?

19 A. Nope.

20 Q. OK. So just hypothesize with me that Amol didn't care
21 about being a coder. Fair to say, then, he wouldn't be upset
22 about being moved out of EDG, correct?

23 A. I can't speak to that.

24 Q. Well, you're the boss. You said you knew the culture. You
25 tell me.

K2dWsch6

Stith - Cross

1 A. I can't speak to Amol's intentions or his thoughts.

2 Q. OK. Well, did you know what Amol's goals were at that
3 time?

4 A. No.

5 Q. Did you know Amol wanted to anyway leave EDG?

6 A. No.

7 Q. Did you know if he cared about remaining in EDG?

8 A. No.

9 Q. How about Mr. Schulte; did you know if he cared about
10 remaining in EDG?

11 A. No.

12 Q. Did you know if he wanted to leave EDG?

13 A. No.

14 Q. Did you know if it would have mattered to him if he left
15 EDG?

16 A. No.

17 Q. So it's fair to say that an action taken against two people
18 would have a different effect on two people, correct? You said
19 you moved both --

20 A. Yes.

21 Q. -- right?

22 Amol seemed unconcerned and just embarrassed at having to
23 be there at all, correct?

24 A. They were both moved within EDG.

25 Q. I understand that. One was moved to RDB and one was moved

K2dWsch6

Stith - Cross

1 to some mechanic group. I'm sorry. I've forgotten that
2 acronym. You will have to forgive me.

3 They were moved to different groups, right?

4 A. They were moved to different branches.

5 Q. Branches, yes.

6 A. Yes.

7 Q. I keep getting that wrong.

8 They were moved to different branches, right? You have no
9 idea, sitting here today or back in April, whether it mattered
10 to either one of them which branch they were sent to?

11 A. No.

12 Q. Right. And it was decided that both should be moved
13 because management thought that even-stein was the best way to
14 go, correct?

15 A. Yes.

16 Q. That's what was best for management, correct?

17 A. That's what was best for the environment in which they were
18 both in.

19 Q. Well, did you separately ask each one of them if it would
20 matter if they were moved? No, right?

21 A. No.

22 Q. Did you ask any one of them if they were truly invested in
23 the projects that they were working on that they didn't want to
24 leave?

25 A. No.

K2dWsch6

Stith - Cross

1 Q. Did you ask them, Hey, listen, have you been working on
2 something for a very long time that would upset you if you were
3 taken off of that project?

4 A. No.

5 Q. OK. And you also testified -- I just want to shift gears
6 for one minute before I forget my train of thought. You
7 testified it was normal to take over access when somebody's
8 moved, correct? Normal practice --

9 A. Yes.

10 Q. Standard operating procedure, so to speak; yes?

11 A. Yes.

12 Q. OK. Do you know when they moved these two individuals
13 whether either or both of them took with them any part of their
14 work with them?

15 A. No.

16 Q. Did you know whether or not they took any part of a tool
17 that they were working on?

18 A. No.

19 Q. Did you know what tools either one of them was working on?

20 A. No.

21 Q. Did you know if somebody sat down and said: Hey, you know
22 what? You're moving projects, but we're going to let you take
23 some of your projects with you so that you can continue working
24 on them?

25 A. No.

K2dWsch6

Stith - Cross

1 Q. Imagine that one of them, or both of them, were told that.
2 Then the standard operating procedure of removing access across
3 the board would not -- or possibly would not -- make sense,
4 correct?

5 A. I can't speak to that.

6 Q. Now, you were shown, on direct, this --

7 MS. SHROFF: May I please have 1046 on the screen.

8 Q. And if we could just look at the "from" line, the top line,
9 that was read to you before. Ready? Up there. Do you see
10 that?

11 A. So, "I was told there would be no written response to my
12 email, so I'm proceeding with my move, assuming it is directly
13 due to my security report."

14 Q. And then the next line says?

15 A. "If this is not the case, then please reply."

16 Q. OK. And I just want to make sure, because we went through
17 these -- everybody, all three of us have a rapid pace of
18 speech.

19 THE COURT: Just ask the question.

20 Q. This email was not sent to you, correct?

21 A. No, it was not.

22 Q. OK. So the email was sent to Mr. Leonis, correct?

23 A. Yes.

24 Q. And do you, by any chance, know if Mr. Leonis replied?

25 A. No.

K2dWsch6

Stith - Cross

1 Q. You don't know, or no, he didn't reply?

2 A. I don't know if he replied.

3 Q. OK. And you didn't reply because you were just carbon
4 copied on it, correct?

5 A. Yes.

6 Q. And there are a lot of people that this man carbon copied,
7 correct? I mean, not carbon copied. I apologize.

8 A. Cc'd.

9 Q. Electronically copied, right?

10 A. Yes.

11 Q. So you do not know if, in fact, that statement or that
12 clause is accurate or not, correct?

13 A. No.

14 Q. You don't know?

15 A. I don't know.

16 Q. Right. So it could be that he was told that there would be
17 no written response, correct?

18 A. Yes.

19 Q. And it could be that he wasn't told that, correct?

20 A. Yes.

21 Q. It's an equipoise. Nobody knows.

22 OK. And then it says, "I'm proceeding with my move,
23 assuming it is directly due to my security report." What
24 security report is he talking about?

25 A. I don't know.

K2dWsch6

Stith - Cross

1 Q. And then it says he is going to be leaving early today,
2 can't complete his move, and he will complete the process
3 tomorrow, right?

4 A. Yes.

5 MS. SHROFF: OK. May I just see the bottom part of
6 this email. No, no. The middle part. I'm sorry.

7 Q. See that part where it says, "I just want to confirm this
8 punishment of removal from my current branch is for reporting
9 to security an incident in which my life was threatened and/or
10 submitting a protective order against Amol, "correct?

11 A. That's what he wrote.

12 Q. That's what he wrote. And you said you did not agree that
13 there was any indication that his life was threatened, correct?

14 A. I did not agree.

15 Q. Right. You did agree, though, that somebody had a
16 protective order, right?

17 A. They'd gone to court.

18 Q. Yes, that's right. So you knew there was a protective
19 order?

20 A. Yes.

21 Q. And do you know if anybody replied to this email of his?

22 A. I don't know.

23 Q. OK. Fair enough. And again, this email is not directed at
24 you; you're just copied on it, correct?

25 A. Yes.

K2dWsch6

Stith - Cross

1 Q. And then if you keep going down, that is just both of these
2 individuals being informed of the change, correct? There's
3 nothing more to it that involves you, right?

4 A. Yes.

5 Q. OK. Now, there comes a point when you, in fact, are
6 emailed, correct, directly by Mr. Schulte?

7 A. Yes.

8 Q. And these emails that were 1046 are dated March 29,
9 correct? And then the one he sends to you is April 6. There's
10 a short gap, right? It's not long, but it's a gap, is that
11 right? Do you have it?

12 A. I don't -- I'm not looking at those ones right now.

13 Q. OK. No. You're right.

14 Is hard copy better for you?

15 A. Fine.

16 THE COURT: The screen doesn't seem to be able to
17 catch up with you, Ms. Shroff.

18 MS. SHROFF: Oh, here it is. 1046's up. There you
19 go. All right.

20 Q. Do you see he sends you this long email, right?

21 A. Yes.

22 Q. Except the last two pages?

23 A. Yes.

24 Q. Right. And at this point, he has involved somebody above
25 his own boss, Sean and Karen, right?

K2dWsch6

Stith - Cross

1 A. Yes.

2 Q. And he's telling somebody that the reason he is going above
3 Karen is because, at least according to his state of mind,
4 Karen isn't listening to him, correct?

5 A. Yes.

6 Q. OK. And he says something about moving desks?

7 A. Well, that's when they were moving to separate branches, I
8 think.

9 Q. Right. And he says that he was told that he had refused to
10 move desks and that he disagreed with that statement or that
11 accusation, correct? He's telling you he thinks it's not true?

12 A. Yes. I'm looking at this note.

13 Q. Correct?

14 A. Yes.

15 Q. OK. Then he says, at the end, or towards the end, "I was
16 told that management does not want anything in writing and that
17 my emails would not be responded to in writing." Do you see
18 this part? There you go. Do you see that?

19 A. Yes.

20 Q. "If that is still the case, I hope that my concerns can be
21 addressed in another way," correct?

22 A. Yes.

23 Q. OK. So as of April 6, he's still telling somebody that
24 somebody's not responding to him in writing, right?

25 A. Yes.

K2dWsch6

Stith - Cross

1 Q. OK. And then he says: "More than anything, I want this
2 situation to go away. I feel like I'm being punished and that
3 confidential information is told to Amol." Right?

4 A. Yes.

5 MS. SHROFF: OK. You can take that down.

6 Q. Now, on direct, you were asked questions about if this was
7 the first time ever that somebody at your level of management
8 had to be made or had to get involved in this level of dispute,
9 correct?

10 A. If it was the first time I had been involved at my level in
11 this type of dispute, yes, at that level.

12 Q. I just assume -- your tenure spanned a long time. Ten
13 years or something, more than ten years?

14 A. As director of the center, my tenure spanned a year.

15 Q. All right. And you personally have never been involved
16 with this level of a dispute, correct?

17 A. As director, no.

18 Q. And had there ever been a time that you can recall where
19 somebody sought a protective order because their concerns were
20 left unaddressed, at least according to them?

21 A. No.

22 Q. OK. Is it fair to say that it was upsetting that two CIA
23 employees had gone to a public court to air this fight?

24 A. One employee chose to go to the court to air the fight.
25 The other did not.

K2dWsch6

Stith - Cross

1 Q. One employee chose to go to court to air the fight. That's
2 correct. Not something the CIA wanted, correct?

3 A. Not something that was typically done.

4 Q. I'm sorry. I apologize, but that really wasn't my
5 question. My question was whether or not that was something
6 that the CIA would want to see, ever.

7 A. I don't know that I can speak for the CIA.

8 Q. Well, you spoke for the CIA for a whole year, right?

9 A. I spoke for the Center for Cyber Intelligence --

10 Q. OK.

11 A. -- for a year.

12 Q. How about that? Let's try that. As the director of the
13 CCI, it would not be something that you would want to see,
14 ever, correct?

15 A. I would not want to see that, ever.

16 Q. Right. By the way, after Mr. Schulte went to court, were
17 you aware that Amol also went to court to respond?

18 A. I think -- I don't recall that.

19 Q. Did Karen not brief you on this?

20 A. I can only speak to what I recall.

21 Q. So --

22 A. I don't recall that.

23 Q. -- you don't recall Karen briefing you on it then?

24 A. I don't recall it.

25 MS. SHROFF: May I just have a moment, your Honor?

K2dWsch6

Stith - Cross

1 THE COURT: Yes.

2 Q. You met with the government, did you not, to prepare for
3 your testimony here?

4 A. I did.

5 Q. And you were actually kind enough to also speak to me,
6 correct?

7 A. I did.

8 Q. Right. And the last time that you met with the government
9 was on February 12. That was yesterday, correct?

10 A. Yes.

11 Q. OK. And who accompanied you to the meeting with
12 Mr. Laroche? Who else was present, do you know?

13 A. I think Dave was present.

14 Q. Who's Dave?

15 THE COURT: Mr. Denton.

16 Q. Oh, Mr. Denton.

17 A. Yeah.

18 Q. Was anybody else also present?

19 A. There was an attorney there as well.

20 Q. What's the attorney's name?

21 A. Christine.

22 Q. And who does she work for?

23 A. She works for the CIA.

24 Q. So you had an attorney from the CIA present with you when
25 the government was prepping you for testimony?

K2dWsch6

1 A. Yes.

2 MS. SHROFF: OK. I have nothing further.

3 MR. LAROCHE: No further questions, your Honor.

4 THE COURT: You're excused, Ms. Stith. Thank you very
5 much.

6 THE WITNESS: Thank you.

7 THE COURT: Watch your step.

8 (Witness excused)

9 THE COURT: OK. As we've agreed before, we won't be
10 sitting on Fridays. That's tomorrow, the 14th. It's
11 Valentine's day. You're going to be off for Valentine's day.
12 Monday is a national holiday, President's Day, so we won't be
13 sitting on Monday either. You're going to have a long weekend,
14 a four-day weekend, so remember my instructions. Don't talk
15 about the case. Don't do any research. Don't listen to any
16 radio or media concentrating on it. Keep an open mind.

17 We'll see you Tuesday morning at 9:00. Thank you very
18 much.

19 (Continued on next page)

K2dWsch6

1 (Jury not present)

2 THE COURT: Please be seated.

3 Anything to take up?

4 MS. SHROFF: No, your Honor.

5 MR. LAROCHE: No, your Honor.

6 THE COURT: Mr. Zas, anything?

7 MR. ZAS: No, sir.

8 THE COURT: All right. See you on Tuesday morning.

9 MS. SHROFF: See you Tuesday.

10 MR. LAROCHE: Thank you, your Honor.

11 THE COURT: We have another matter.

12 (Adjourned to February 18, 2020, at 9:00 a.m.)

INDEX OF EXAMINATION

Examination of:	Page
-----------------	------

MICHAEL

Cross By Ms. Shroff1264
-------------------------------	-------

MICHAEL BERGER

Direct By Mr. Kamaraju1335
----------------------------------	-------

Cross By Mr. Branden1410
--------------------------------	-------

Redirect By Mr. Kamaraju1429
------------------------------------	-------

BONNIE BENNETT STITH

Direct By Mr. Laroche1435
---------------------------------	-------

Cross By Ms. Shroff1455
-------------------------------	-------

GOVERNMENT EXHIBITS

Exhibit No.	Received
-------------	----------

3002, 1305-1 through 1305-101342
--	-------

1306-1, 1301-1 through 1301-4B, 1302-11342
--	-------

1304-1 through 1304-31342
---------------------------------	-------

17041344
----------------	-------

DEFENDANT EXHIBITS

Exhibit No.	Received
-------------	----------

F1275
-------------	-------